Routing and Mobility Strategies for Mobile Ad Hoc Networks

Mohammed Husein Alchaita

Wireless & Multimedia Communications & Signal Processing Research Group

School of Engineering and Technology

Faculty of Computing Sciences and Engineering

De Montfort University, United Kingdom

A dissertation submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy

September 2006

Declaration

No part of the material described in this thesis has been submitted for the award of any other degree or qualification in this or any other university or college of advanced education.

Mohammed Alchaita

Dedication

To my parents
who deserve special recognition
for their endless support all the way through my life.

To the memory of my father
who passed away during my research period
without being able to see him,
never ever be forgotten.

Acknowledgements

First and foremost, my deepest gratefulness goes to GOD for all his blessings without which nothing of my work would have been done. I would also like to express my sincere gratitude to my supervisor Professor Marwan Al-Akaidi at De Montfort University, United Kingdom, for his guidance, ideas, invaluable directions and support throughout my research study. Without his contributions, this research would not have been possible. I am deeply indebted to him for his insights and suggestions to the thesis topic and for invaluable supervision at various stages of my work. He has helped me in many ways and has developed my academic thinking, problem solving and technical writing which will be very helpful in my future work and research. I feel extremely lucky to have him as my supervisor, who is always dedicated to the success of his students. Grateful acknowledgement is also made to my second supervisor Mr. Jon Ivins at De Montfort University, United Kingdom, for his ideas, encouragement, and support. His insightful assistance has greatly helped me to improve the quality of this work. I am grateful for the support and assistance from all members of the WMCSP (Wireless & Multimedia Communications & Signal processing) research group, who have given me a sense of belonging as a group. I am also thankful to my colleagues at the WMCSP Research group. I have benefited from many fruitful discussions and collaboration with them. I am also deeply indebted to all members of my family for their endless encouragement and without which I could not cope with the anxiety and stress.

Last but not least, I would like to express my gratefulness to my colleagues in my work place at SSRC centre in Damascus, Syria, for their support. In addition, special thanks are made to Dr. Nizar Alhafez and Dr. Said Desouki, at SSRC for their advice, help, and cooperation.

Mohammed Alchaita

Leicester, United Kingdom **September 2006**

Abstract

Mobile Ad hoc NETworks (MANET) are envisioned to become key components in the architecture of the next generation network. In contrast to wired and cellular networks, a MANET is an infrastructureless network that does not depend on any established infrastructure or centralised administration such as a base station. It is an autonomous system of wireless mobile nodes that move freely, randomly and organise themselves arbitrarily. Therefore, the network topology of an ad hoc network is dynamic in nature and may change rapidly and in unpredicted manner. Hence, the intercommunications among nodes are changing continuously. Generally, communication between a source node and a destination node in MANETs are established through multiple intermediate nodes. As a result, any link breaks between any two directly communicating nodes of the established path will result in a break of the complete connection between the source and the destination nodes.

In addition, the mobility of nodes results in route loss, poor longevity of established routes, asymmetric communications links, increase in the control traffic overhead and affects the performance of the routing protocol. Moreover, using a number of routing parameters for routing such as geographical location, speed, and signal strength requires a number of resources to provide these parameters. These resources are unlikely to be always available at the same time.

The aim of this research is to develop three new routing approaches for mobile ad hoc networks within the context of the previously described situations. One objective of developing these approaches is to study the behaviour of a routing protocol when only the "self-dependent" parameter exists for routing information. Other information is absent in the network, such as location information, speed, etc. Another objective is to exploit the mobility of nodes to establish long-lived routes by using the heading direction information of mobile hosts. As third objective, the scope of route requests is to be limited in order to reduce the overhead in the network. The three new approaches developed in this thesis are called Heading direction Angle Routing Protocols. The fist two of these protocols are called HARP1 and HARP2.

The third approach, called HARP3, considers that the geographical location of nodes is available to the network, and hence combines the heading direction of nodes with its position information in setup routes.

A new Adaptive Centralised Location Service (ACLS) routing protocol is presented in this thesis, which tracks mobile node locations. ACLS is an adaptive centralised location service that runs on the mobile nodes themselves without the need for a fixed infrastructure. The main objectives of ACLS are:

1) To reduce the time spent on looking for a server that has information about the position of a required node.
2) To reduce the path length between the nodes and their servers, which are updated with the location information of these nodes.
3) To reduce the path length between the node that requests the location information of another node, and a server node that has this information.
4) To find a solution for the two types of failure caused by node mobility, which already occurs in most existing location service approaches. These failures are: a location server may have out-of-date information, and a server may move out of its current location.

Several optimizations have been implemented in ACLS algorithm in order to improve its efficiency and functionality of providing the requested location information as most accurate as possible.

The concepts of this research were validated by tests carried out on simulation-based approach. The main outcome of this research is the development and implementation of the three HARPs routing protocols (HARP1, HARP2, and HARP3), as well as the ACLS location service routing protocol. HARP approaches have improved the route lifetime and reduced the control overhead and the effect of flooding in the network besides decreasing the effects of mobility. ACLS has fulfilled all the objectives and aims mentioned above. The main result of ACLS is that it is scalable with the network size, speed and mobility of nodes. Case studies and applications have then been investigated to demonstrate the validity of the proposed methodology and environment.

Table of Contents

List of Figures

List of Tables

Abbreviations

ABR	Associativity-Based Routing
ACK	Acknowledgement
ACLS	Adaptive Centralised Location Service
AEED	Average End-to-End-Delay
AODV	Ad hoc On-demand Distance Vector
BRP	Bordercast Resolution Protocol
CBR	Constant Bit Rate
CBRP	Cluster Based Routing Protocol
CEDAR	Core Extraction Distributed Ad hoc Routing
CGSR	*Cluster-head Gateway Switch Routing*
ERDP	the Efficiency Ratio of Data Packet delivery
DBF	Distributed Bellman-Ford
DCF	Distributed Coordination Function
DPDR	The Data Packet Delivery Ratio
DREAM	Distance Routing Effect Algorithm for Mobility
DRP	Dynamic Routing Protocol
DSDV	Destination Sequence Distance Vector
DSR	Dynamic Source Routing
DV	Distance Vector
FORP	Flow Oriented Routing Protocol
FP	Forwarding Protocol
FSR	Fisheye State Routing
GLS	Grid Location Service
GPS	Global Positioning System
ITS	Intelligent Transportation Systems
LANDMAR	Landmark Routing Protocol
LAR	Location-Aided Routing
LBRR	Local Broken Route Repair
LCC	Least Cluster Change
LL	Link Layer
LRR	List of Route Records
MAC	Medium Access Control
MACAW	Medium Access Protocol for Wireless LANs
MANET	Mobile Ad hoc Network
MCDS	Minimum Connected Dominating Set
MN	Mobile Node
MR	Magneto Resistive
MRL	Message Retransmission List
NAM	Network AniMator
NS2	the Network Simulator 2
OLSR	Optimised Link State Routing Protocol
OTcl	Object Tool Command Language
PAN	Personal Area Networking
QoS	Quality Of Service
RD	Research and Development
RERR	Route ERRor
RREP	Route REPly
RREQ	Route REQuest

GPSR	Greedy Perimeter Stateless Routing
GSR	Global State Routing
HARP	Heading-direction Angles Routing Protocol
HARP1	the first Heading-Direction-Based Routing Protocol
HARP2	the second Heading-Direction-Based Routing Protocol
HARP3	the third Heading-Direction-Based Routing Protocol
HDA	Heading Direction Angle
IARP	Intrazone Routing Protocol
IEEE	Institute of Electrical and Electronics Engineers
IERP	IntErzone Routing Protocol
IETF	Internet Engineering Task Force
IfQ	Interface Queue
ZRP	Zone Routing Protocol
RWP	Random WayPoint model
SAR	Search And Rescue
SRDLQRP	Success Rate of Delivering the Location Query Request Packets
SRDLUP	Success Rate of Delivering the Location Update Packets
SSA	Signal Stability-based Adaptive routing
SST	Signal Stability Table
STAR	Source Tree Adaptive Routing
SUM	Server Update Message
TCL	Tool Command Language
TORA	Temporarily Ordered Routing Algorithm
TTL	Time To Live
WRP	Wireless Routing Protocol
ZHLS	Zone-Based Hierarchical Link State

Publications

1. **M Al-Akaidi and M Alchaita, "A New Approach to On-demand Routing Protocols in Mobile Ad hoc Networks", London Communications Symposium (LCS 2004), University College London, London, UK, 2004**

2. **M Al-Akaidi and M Alchaita, "NEW HEADING DIRECTIONAL ANGLE ROUTING PROTOCOLS FOR MOBILE AD HOC NETWORKS", IEE, Fifth International Conference on 3G Mobile Communication Technologies, 18 – 20 October, London, Uk.2004.**

3. **M. Alchaita, M. Al-Akaidi, "EXPLOITING MOBILITY FOR LONGIVITY OF ROUTES IN AD-HOC WIRELESS NETWORKS", PREP 2005, University of Lancaster, 2005.**

4. **M Al-Akaidi and M Alchaita,"MOBILITY-AWARE ROUTING ALGORITHM FOR MULTI- HOP AD-HOC WIRELESS NETWORKS", SSD'05, the Third IEEE International Conference on Systems, Signals & Devices, Sousse, Tunisia, 2005**

5. **M. Alchaita, M. Al-Akaidi, J. Ivins, "New On-demand Routing Approaches for Ad Hoc Networks", PGNet 2005, sixth annual postgraduate symposium, the convergence of telecommunications, networking and broadcasting, 27th-28th June 2005, Liverpool, UK**

6. **M. Alchaita, M. Al-Akaidi, M. Aziz, "APPLICATION OF A NEW ROUTING PROTOCOL IN TELECARE SYSTEM", PGBIOMED05, IEEE EMBSS UKRI Postgraduate Conference on Biomedical Engineering and Medical Physics, 18-20 July 2005, University of Reading, UK.**

7. **M. Alchaita, M. Al-Akaidi, J. Ivins, "Service-Aware Routing Protocols (SARP): Exploiting mobility with loose delay constraints in ad hoc networks", MESM'2005, The 7th International Middle Eastern Multiconference on Simulation and Modelling, The University of Porto, Portugal, 24-26 October 2005**

8. **M. Al-Akaidi, M. Alchaita, J. Ivins, "HEADING ROUTING PROTOCOLS: MOBILITY-BASED ROUTING FOR AD-HOC NETWORKS", 3G 2005, Sixth International Conference on 3G and Beyond - 3G 2005, 07-09 November 2005, The IEE, Savoy Place, London, UK.**

9. **M. Alchaita, M. Al-Akaidi and J. Ivins, "MOBILITY-BASED ROUTING FOR MOBILE AD HOC NETWORKS", The International Middle Eastern Multiconference on Simulation and Modelling (MESM'2006), August 28-30 2006, Mercure Romance Hotel, Alexandria, Egypt.**

10. **M. Al-Akaidi, M. Alchaita, J. Ivins, "On Link Longevity and Mobility in Self-Dependent Multi–Hop Mobile Environment", Submitted to IEE Proceedings Communications, 09-May-2006.**

11. **M. Al-Akaidi, M. Alchaita, J. Ivins, "Link Longevity and Mobility in Self-Dependent Multi-Hop Mobile Environments", Submitted to the International Journal of Mobile Communications, July 21, 2006**

Chapter 1
Introduction

1.1 Background and Motivation

This section presents the definition of wireless mobile ad hoc networks and its challenges, and elaborates on one of the most challenging and interesting research areas in MANET; routing. It should be noted that the terms “node” and “host” are used interchangeably throughout the thesis. This is because in ad hoc networks each mobile node acts as a host and a router. In addition, in some literature, a mobile node is called a host.

1.1.1 Ad hoc Networks

The study and development of infrastructureless wireless networks have been very popular over the recent years. Mobile Ad hoc Networks (MANETs) belong to the class of these networks which does not require the support of wired access points or base stations for intercommunication. A mobile ad hoc network, unlike a static network, has no infrastructure. It is a collection of mobile nodes where communication is established in the absence of any fixed foundation. The only possible direct communication is between neighbouring nodes. Therefore, communication between remote nodes is based on multiple-hop. These nodes are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. Each mobile node acts as a host and a router, relaying information from one neighbour to others. For example, in Figure 1-1, nodes A and D must enlist the aid of nodes B and C to relay packets between them in order to communicate.

The task of finding and maintaining routes in mobile ad hoc networks is nontrivial [1, 2] for two reasons: the first reason is the node mobility causes frequent unpredictable topology changes. The second reason is that establishing a route between end-points requires routing over multiple-hop paths whose end-points are likely to be in motion.

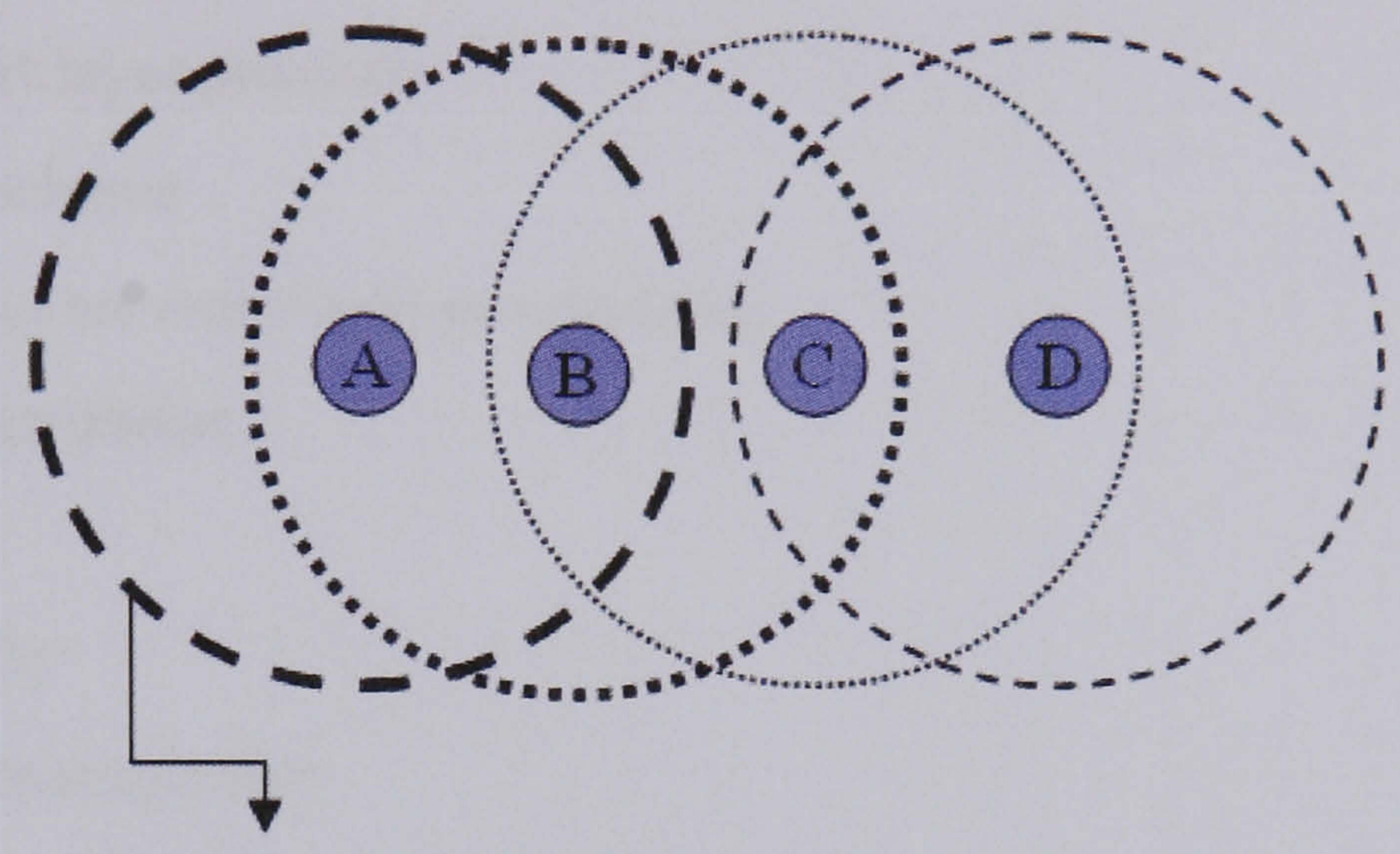


Figure 1-1: An ad hoc network of four nodes, the node *A* communicates with node *D*

Since ad hoc networks could be deployed rapidly without the support of a fixed infrastructure, they can be used in the situations where temporary network connectivity is needed. For example, conferences, meetings, crowd control, shared whiteboard application (office workgroup), multi-user games, robotic pets, home wireless networks, office wireless networks, search and rescue, disaster recovery and automated battlefields. These environments naturally do not have a central administration or infrastructure available.

1.1.2 Challenges in Ad hoc Networks

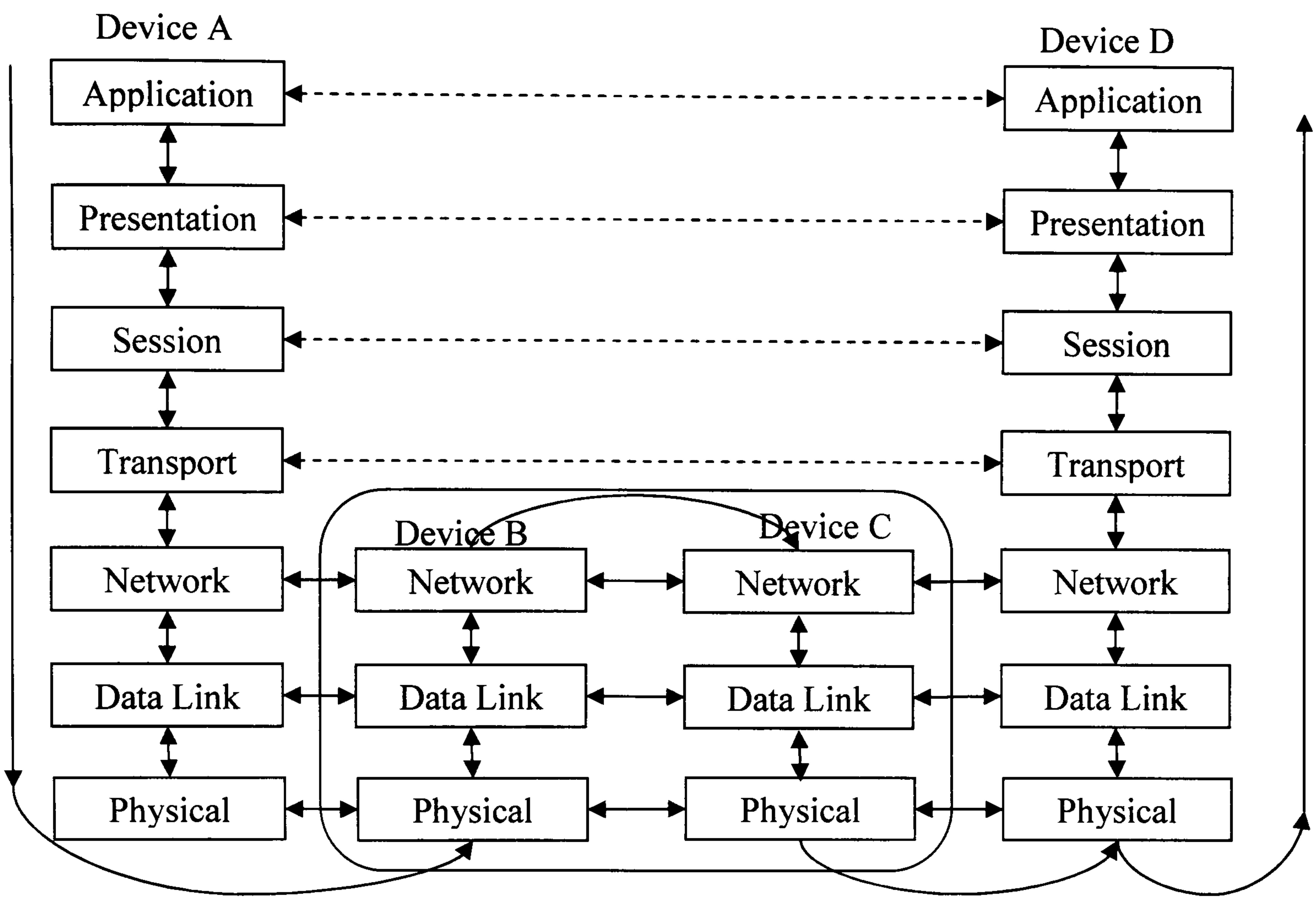
The main challenges in the design and operation of MANETs come from the lack of a centralised entity (infrastructureless) such as base stations, access points and servers, the possibility of rapid node movement and the fact that all communication is conducted over the wireless medium. Due to the unique characteristics of wireless ad hoc networks, the major issues that affect the design, deployment and performance of an ad hoc wireless system and that are interesting research areas in MANETs are as follows [3]:

- Routing
- Mobility
- Medium access scheme
- Multicasting
- Internetworking
- Transport layer protocol
- Pricing scheme
- Quality of service (QoS) provisioning
- Self-organization
- Security
- Reliability
- Energy management
- Addressing and service discovery
- Scalability
- Deployment considerations

1.1.2.1 Wireless Ad Hoc Network Layers

The Open Systems Interconnection (OSI) reference model proposed by the International Organisation for Standardisation (called ISO) consists of seven layers [3], namely, the physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and the application layer (Figure 1-2). Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer over the channel to the next station then back up the hierarchy. The OSI reference model was never implemented in reality because it had many layers that made this model very complex and difficult to implement efficiently. The session and presentation layers were not required for most applications.

Each layer in the model is assigned specific tasks [3]. The first and lowest layer is the physical layer. It may need to adapt to rapid changes in wireless links characteristics and mobility. The physical layer deals with raw bits. It is responsible for bit encoding, determining the voltage to be used for transmitting the bit stream over the physical medium and the time duration of each bit. It is also concerned with the physical



specifications of the devices such as connectors and cables.

Figure 1-2: The communication between the node *A* and the node *D*

The second layer is the data link layer. The functions of the data link layer are to coordinate the access of multiple nodes to a shared (wireless) medium, to ensure error-free transmission of data over a physical link and to take into account the requirement of time synchronization. The data link layer is also responsible for minimizing collisions arising due to simultaneous transmissions by multiple nodes, maximizing throughput, allowing fair access and the use of directional antennas. The data link layer has to solve the problems of hidden and exposed terminals.

The third layer is the network layer, where this research area is concentrated. it is responsible for routing data packets from the source node to the destination node that the data packets belong. Therefore, the network layer has to determine and distribute information used to set up routes between sources and destinations in a way that maintains efficiency when links change frequently. The network layer needs to provide IP addresses to end hosts, to minimise signalling overhead of the control packets required for route establishment and setup routes that support requested QoS and scalability.

The fourth layer is the transport layer. The main objectives of the transport layer protocol include handling delay and packet loss statistics that are very different from wired networks, segmentation and reassembly of packets, setting up and maintaining end-to-end connections, reliable end-to-end delivery of data packets, end-to-end error recovery, congestion control and flow control.
The session and presentation layers are not required in all networks.

Finally, the application layer, it enables the user to access the network. The main role of this layer is to handle frequent disconnection and reconnection with peer applications and to supports data transmission and services between users such as electronic mail, and remote file access and transfer.

1.1.3 Challenges in Routing and Mobility in MANET

The most challenging and interesting research area in MANET is routing. Since routing is a demanding task and is a fundamental requirement for all other research areas in ad hoc networks, it has received tremendous attention from researchers. On the other hand, mobility is a very important factor affecting the performance of the routing protocol. Therefore, the research work in this thesis focuses on routing and mobility in mobile ad hoc networks.

The essential functions of routing protocols include finding a feasible data packet path from a source node to a destination node. It also includes determining and exchanging the routing information required for establishing the routing path, detecting the path breaks, re-establishing or repairing the broken paths and minimizing bandwidth utilization. All these functions have to be performed without generating unnecessary overhead control messages. Control messages must be generated only when necessary and have to be exploited efficiently to deliver data packets. Reducing control message overhead and the effect of flooding reflect the efficiency of routing protocols in terms of bandwidth and energy consumption.

Routing protocols designed for traditional wired networks cannot be directly applied in wireless ad hoc networks due to the unique characteristics of these networks. These characteristics are mobility, highly dynamic topology, power consumption, bandwidth-constrained, absence of infrastructure and limited physical security. Consequently, designing efficient routing protocols is a fundamental challenge and many different routing protocols have been developed for MANET over the past several years [2], with respect to certain metrics and based on different salient characteristics and properties. Examples of metrics and characteristics are power consumption, link state, security, etc.

It is necessary to investigate the applicability of existing ad hoc routing protocols and to determine which ones are suitable for a given application. It is important to determine how to select the appropriate routing protocols for such applications due to the very diverse requirements of the applications and the unpredictable nature of ad hoc networks. This has led to the development of many different routing protocols for MANETs. Each author of each proposed protocol claims that the strategy proposed provides an improvement over a number of different strategies considered in the literature for a given network scenario. Therefore, it is quite difficult to determine which protocols may perform best under a number of different network scenarios, such as increasing node density and traffic.

The performance of mobile ad hoc networks is related to the efficiency of the routing protocol in adapting to changes in the network topology due to mobility of the nodes [4, 5]. With increasing mobility of nodes, the rate of link failure and the activation of broken links increase, which consecutively increase both the congestion due to traffic backlogs, and the volume of control traffic required to maintain routes. Thus in order to achieve adaptive routing responsiveness and efficiency, the main goal of designing a protocol has to be the diminution of reaction to mobility [6]. The research in this thesis concentrates on achieving this goal by designing novel routing protocols.

1.2 Problem Description and Research Goal

Many protocols have been proposed for mobile ad hoc networks, with the aim of achieving efficient routing [2, 7-11]. These protocols differ in the approach used for searching for a new route and/or modifying a known route when hosts move. In designing routing protocols for ad hoc networks, it is essential to maintain the flow of control packets between communicating nodes as well as establishing new links. However, the flow of control packets should be kept to a minimum. This is because increasing the number of control broadcast packets by flooding is very costly and results in serious problems. Such as generating excessive redundant control message overhead, contention and collision. The latter is due to triggering a huge number of packet forwarding that ultimately results in the breakdown of the entire network [12]. Flooding is adopted by many routing protocols, such as Ad hoc On-demand Distance Vector (AODV) [11] and Dynamic Source Routing (DSR) [13] protocols. These conventional routing protocols used in ad hoc networks flood a route request packet to construct a route.

The mobility of nodes in a MANET is a prominent characteristic. It is the main factor [6] affecting topology changes and route invalidation in mobile ad hoc networks. Several routing problems are caused by mobility such as, frequent breaking of the wireless link, packet collisions, short lifetime of the established routes, transient loops, stale routing information and asymmetric communication links. These problems increase the signalling overhead required to establish routes between sources and destinations and thus affecting the performance of routing protocols.

In some situations, where the Global Positioning System (GPS) is utilised by routing protocols to determine the geographical location of nodes, the GPS is not operating well (or even not available at all) such as when the host is in an underground or in a tunnel.

Therefore, the need for alternative routing information to perform the routing functions is crucial to maintain these functions. In addition, in some ad hoc network applications, the nodes usually move in roughly similar speeds such as people on the street. Moreover, using additional information in routing requires additional resources to provide this information (speed, location, signal strength, etc). These resources are most likely to be unavailable all together and if one of these resources is absent, the whole task of routing will fail. Some of the approaches proposed in this thesis utilize the most important "self-dependent" parameter used in such applications, which is the heading direction of the nodes.

Many proposed routing protocols for mobile ad hoc networks rely on geographical information for forwarding packets to the final destinations such as Location-Aided Routing (LAR) [1, 14], Zone-Based Hierarchical Link State (ZHLS) [15], Flow Oriented Routing Protocol (FORP) [16], and Greedy Perimeter Stateless Routing (GPSR) [17, 18].

A location service is combined with and used by location-based routing algorithms to provide the source node (sender) with the location information for the required destination node in a mobile ad hoc network. The sender node then includes in the packets, addressed to the destination, the provided position of the destination. The location service can be described as a mechanism for a node to track the location of other nodes in the network topology. In this thesis, a new adaptive location service approach is proposed in order to overcome some of the drawbacks associated with the existing location service algorithms. The main objectives of the proposed location service are:

- To reduce the time spent on looking for a server that has information about the position of a required node.
- To reduce the path length established from a requester node to a server node.
- To find solutions for the two types of failure caused by node mobility, which occurs in most of the already existing location service approaches. These failures are:
    - A location server may have out-of-date information
    - A server may move out of its current location.

Regarding the above discussion, the aim of the research in this thesis is to find solutions to the following problems:

- How to design new adaptive mechanisms/algorithms/approaches of routing for mobile ad hoc networks.
- In ad-hoc networks, there are no centralised entities infrastructure, (such as the base stations in a cellular network), where these entities act upon the function of coordination. The lack of these infrastructures in ad hoc networks requires an alternative mechanism to perform this function such as distributed algorithms. Therefore, the question arisen here is how to accomplish the new proposed adaptive mechanisms of routing by means of distributed algorithms?
- How to minimise the control packets overhead through these distributed algorithms.
- How to achieve a decisive protocol design via the diminution of reaction to the mobility of nodes.
- How to handle the frequent changes in the network topology.
- How to exploit mobility of nodes to provide and maintain a long-lived multi-hop path between two communicating nodes, and minimise the frequent breaking of the wireless link.
- How to change mobility of nodes in mobile ad hoc networks from being hindrance to be helpful.
- What is the alternative routing information to perform the routing functions when the ad hoc network is short of external information such as GPS, and how to utilise this information.
- What are the requirements for designing a new adaptive location service in order to overcome the failures of a central server accompany with the centric server location service algorithms? In addition, how to achieve these requirements.

1.3 Approaches and Accomplishments

This research investigation started from the fact that mobility makes routing in ad hoc networks more challenging to adapt to changes in the network. The mobility of nodes can also be useful in enhancing the performance of routing in ad hoc networks. This fact is contrary to the common belief that mobility is a burden to the network. In addition, investigating the use of a minimum amount of routing information in routing protocols is another aim behind this research because in certain situations, external routing information (provided by external resources) may not be available. Therefore, three novel on-demand routing schemes are proposed that exploit the mobility of nodes to answer the questions mentioned earlier in section 1.2. One of the aspects to be exploited is the heading direction of the node. In the proposed schemes, establishing a route is dependant on selecting only a small subset of the network nodes based on its Heading Direction Angle (HDA). Specifically, this research starts by proposing a new on-demand routing protocol described in the literature as *Al-Akaidi-Chaita* scheme 1 [19, 20]. The principal ideas of this protocol are:

- To limit the flooding of the Route Request (RREQ) packet required to establish a route between a source node and a destination node, to a small number of nodes rather than request all the nodes in the network to flood this packet.
- Starting from the source node, each node selects the downstream node from neighbour nodes, which the RREQ packet will be forwarded to, based on the heading direction angle of this node. This way of selection continues until RREQ packet reach to the intended destination or the lifetime of RREQ packet is expired.
- The established route is based on providing and maintaining, a robust and long-lived multi-hop path between two communicating nodes. This leads to minimising the frequent breaking of the wireless link.

As the next node in the path is selected to be of similar/near heading direction to the previous node, the RREQ packet might not meet the destination. Hence, the RREQ packet for finding the path is triggered again in another direction, different from the previous selected direction. Therefore, this protocol is efficient in such situations where nodes move in the same heading direction [19], or the nodes' decisions on movement depend upon the other nodes in the group. This protocol is also efficient in situations where nodes are uniformly moving forward in a particular direction such as vehicles on the highway. In addition, this protocol, if implemented in other existing protocols, will enhance their performance in terms of long-lived route.

To increase the chance of finding the destination node from the first try of transmitting the route request, an improved version of the first protocol was designed. It has a better probability of finding the destination and it is denoted as *Al-Akaidi-Chaita* scheme 2 [19, 20]. The main idea of this protocol is to propagate the RREQ packet by the source node to more than one neighbouring nodes (the number of packets propagated by the source to its neighbours is equal to the number of direction zones and only one neighbour from each zone is selected). Then each node from these nodes will select one next node according to the heading direction angle of this node. This protocol increases the probability of finding the destination while reducing the effects of flooding, maintains a robust, long-lived path between the source and destination nodes and minimises the failures of the wireless link.

In order to reduce the number of selected nodes in the second routing protocol without affecting the performance of the protocol and to exploit the mobility of nodes to reduce the topology changes of the network, additional routing information is required. To determine the location of the destination more precisely, the geographical locations of nodes and destination is used. Hence, the third on-demand routing protocol is designed and denoted as *Al-Akaidi-Chaita* scheme 3 [19, 20]. In this scheme, the use of external routing information (such as GPS) is investigated. This scheme is assisted by the location information that could be provided by the (GPS) [21, 22]. The core idea of this protocol is that in order to setup a route, each node selects only one next node from its neighbour vicinity according to its geographical locations and its HDA.

During the period of the research in this thesis, a general framework for an important application of mobile ad hoc networks [23] has been proposed as an application to this research. This framework is about implementing and using mobile ad hoc network in the telecare system in order to help elderly people to get better treatments. The proposed framework [23] for telecare combines live audio, two-way video connection and monitoring technology equipped with a variety of medical peripherals, all aimed to create a flexible, and user friendly patient-specific home Telecare Systems. This framework enables elderly patients at home to personally, carry out tests or taking measurements for so many parameters related to the disease or to the body condition (e.g., blood pressure, temperature, electro cardio gram, etc.). This information will be transmitted over the air interface using a wireless communication device to the specialised health centres to remotely interact from a variety of locations.

Finally, in the third proposed routing protocol, the source requires information about the location of the destination node. The location service protocols offer this type of information. Consequently, a new Adaptive Centralised Location Service (ACLS) algorithm is proposed. This algorithm satisfies all of the main characteristics of location service in terms of the scalability. These characteristics are:

- Spreading the maintained location service information evenly over many nodes to ensure the availability of this information in case of the failure of any node that maintains the information, therefore,
- The failure of a node should not affect the reachability of other nodes.
- The location information storage and the cost of communication of the location service should grow as a small function of the total number of nodes.
- The time of searching for a location of node should be as minimum as possible.
- The availability of up-to-date location service at any time.

1.4 Contribution

The key contributions of the routing protocols and mobility exploitation strategies for wireless ad hoc networks presented in this thesis are summarised as follows.

The three proposed routing protocols convert mobility from being a hindrance to be helpful. Minimizing connection breakdown, controlling packet overheads and extending the route connection time are considered crucial factors in ad hoc networks. Therefore, in the proposed algorithms the use of the HDA of nodes was examined to select a robust and long-lived route to destination. In addition, the use of minimum routing metrics used for establishing routing functions was investigated for use in an ad hoc network which is lacking routing information. The use of heading direction of nodes when the external routing resources are available was also investigated. This external information is the geographical information of nodes that could be provided by GPS.

Results show that selecting the nodes according to their HDA will overcome the effect of flooding techniques and overhead in the network. These results can be considered to be mechanisms of solutions to problems raised earlier in section 1.2. Other existing routing protocols for mobile ad hoc networks could apply to the proposed techniques in order to improve the performance of these protocols in terms of elongating the lifetime of the communications.

In addition, the location service algorithm has to satisfy the main characteristics of location service mentioned earlier. Moreover, this algorithm has also to be adaptive with the topology changes. Finding a solution for the two types of failure caused by node mobility is imperative. These failures occur in existing static central server of location service. In order to achieve these requirements and in regards to the drawbacks of static central server approaches of location service, a new adaptive location service algorithm that satisfies all required characteristics has been developed.

1.5 Thesis Outline

This thesis is organised into 10 chapters. The following paragraphs present the outlines of the remaining chapters of this thesis.

Chapter 2 presents an overview of the state-of-the-art ad hoc routing protocols and mobility. It provides classifications of ad hoc routing protocols and gives a general idea and some examples for each class of these classifications. This chapter also describes an overview on the mobility in ad hoc wireless Networks. The chapter is focused on the following aspects: (1) effects of mobility on routing, (2) Mobility Models, and (3) Mobility Prediction.

Chapter 3 includes related works, research methodology, the key idea of heading direction and the mechanism principle of heading direction routing. Moreover, this chapter establishes models for ad hoc networks and starts by defining the system model and listing the assumptions adopted in developing the new algorithms. This chapter also describes the general network model, mobility model, traffic model and general system model that includes the format of all types of messages used in these algorithms.

Chapter 4 presents the design and development of the first proposed Heading-Direction-Based Routing Protocol (HARP1), including the evaluation and simulation results based on the Network Simulator package NS2.

Chapter 5 demonstrates the second proposed Heading-Direction-Based Routing Protocol (HARP2). It also presents the validation and simulation results based on the network simulator NS2.

Chapter 6 describes the idea of the third proposed Heading-Direction-Based Routing Protocol (HARP3). It also describes the simulation environment used to conduct the studies described in relation to this proposed routing protocol and it explains the metrics against which the protocols being studied are evaluated.

Chapter 7 introduces comparative analysis of the three proposed routing protocols by comparing the performance of these routing protocols with each other and with the AODV routing protocol. This is because AODV is a conventional on-demand routing protocol and the three proposed routing protocols are also on-demand routing protocols.

Chapter 8 introduces a new adaptive location service for geographical-based routing protocol. This chapter includes the motivation, early work on location service, the description of the new Adaptive Centralised Location Service (ACLS) and the evaluation and validation results.

Chapter 9 demonstrates an important case study and a significant application of the proposed routing protocols. This includes a proposed framework for telecare system, and inter-vehicles ad hoc System.

Chapter 10 presents the conclusions of the work carried out the thesis and outlines recommendations for future work.

Chapter 2

State of the Art of Ad hoc Routing Protocols and Mobility

Designing and developing efficient and reliable routing protocols are essential challenges in mobile ad hoc networks. This is due to the specific characteristics of mobile ad hoc networks, including mobility, power consumption, bandwidth constraints and dynamic topologies. Over recent years, a number of different routing protocols for ad hoc networks have been developed and proposed with respect to certain routing metrics and based on different salient characteristics and properties [1, 2, 5, 9-13, 24, 25]. Due to the variety of applications and the unpredictable nature of ad hoc networks, it is important to determine which protocols are suitable for a given application.

Generally, the routing protocol is used by a node that works as a router to determine the appropriate path over which data is transmitted. This protocol specifies how these nodes in the network share information with each other and report changes. Routing protocols used in traditional wired networks cannot be directly applied in mobile ad hoc wireless networks for two reasons. The first reason is the absence of centralised administration established by infrastructure such as base stations or access points. The second reason is the dynamic topology of ad hoc network, bandwidth constrained links and energy constrained nodes.

Investigations of routing problems in ad hoc networks have begun by enhancing the performance of existing routing protocols of wired networks to be suitable for mobile ad hoc networks. This enhancement has to overcome the problems associated with the two main algorithms commonly used in wired networks. These two algorithms are referred to as link-state and distance vector algorithms [26]. In these algorithms, the main drawback is that they do not scale in large ad hoc networks due to the periodical broadcasting. The broadcasting utilises a flooding strategy and frequent route updates in large networks results in consumption of the available bandwidth and an increase in channel contention.

Due to proposing and developing a variety of routing protocols for ad hoc wireless networks in the recent years, different classifications of routing protocols can be raised. In this chapter, the strengths and weaknesses of current routing protocols are investigated and how the findings can be used to find a solution for these weaknesses is discussed. This chapter also shows that the discussion presented here will assist application developers in selecting the appropriate protocols for their applications. This study also paves the way for further research to be done in order to improve the performance of these protocols. A detailed discussion on current routing protocol classifications are given below.

2.1 Classifications of Current Routing Protocols

Routing protocols proposed for mobile ad hoc wireless networks can be generally classified into different categories based on routing strategy. These categories are Proactive, On-demand, and Hybrid. Another classification can be based on packet casting, which includes Unicast, Anycast, Multicast, Broadcast, and Geocast. Moreover, routing protocols can be classified according to path selections and addressing topology. Path selection group includes path selection using past history, and path selection using prediction. The addressing topology group includes flat addressing topology and hierarchical addressing topology. These categories are not mutually exclusive since some routing protocols could be classified in more than one category. The work in this thesis is related to the routing protocols based on routing strategy and geographical location. Hence, only these two categories will be discussed. Researchers interested in other remaining categories and who needs details about other routing protocols can refer to [2, 3, 24].

2.1.1 Routing Protocols Based on Routing Strategy

The routing protocols group, as mentioned earlier, can be classified into three main groups; proactive (periodic), reactive (on-demand), and hybrid [2, 3, 24].

2.1.1.1 Proactive Routing Protocols

The proactive routing protocol is also called the table-driven routing protocol since each node maintains one or more tables to store the network topology and routing information. This information is updated by periodically exchanging routing information, by flooding the routing information in the whole network. The difference between different proactive routing protocols depends on the method of detecting and updating the routing information and the type of information maintained in the routing tables. Distance vector and link-state routing protocols are types of this category. Distance vector protocols are based on the classical Bellman-Ford routing algorithm [27, 28] where each node maintains a list of all destinations and number of hops to each destination. As a result, these protocols do not perform well in such networks where the nodes are mobile because of the slow convergence and count-to-infinity problem[1] (If a certain kind of link failure occurs in a routed network, the result is that the algorithm tries to count the shortest paths to infinity). Therefore, a number of proposed protocols have modified and enhanced the distance vector algorithm to be suitable for mobile ad hoc network. Examples of such protocols: Destination Sequence Distance Vector (DSDV) routing protocol [29], Wireless Routing Protocol (WRP) [30, 31]. In addition, different routing protocols are proposed based on link state algorithms such as Optimised Link State Routing (OLSR) protocol [32], Fisheye State Routing (FSR) protocol [33, 34], Source Tree Adaptive Routing (STAR) protocol [35], and Global State Routing (GSR) protocol [36].

Some examples of protocols that belong to the table-driven category are elaborated on in next section. The aim of discussing these examples is to understand the way in which proactive or table-driven routing protocols update routing information and establish the path between the source node and the destination node in the network. These examples also highlight the difference between these protocols and other categories of routing protocols.

2.1.1.1.1 Destination-Sequenced Distance-Vector

[1] The algorithm counts the number of nodes that connect the source with the destination, if a link between any two of these node is broken, the algorithm will consider the number of nodes is undetermined. This is called count-to-infinity problem

The Destination-Sequenced Distance-Vector (DSDV) algorithm [29] is an outcome of the modification of the Distributed Bellman-Ford (DBF) algorithm [27, 28]. It guarantees faster convergence and resolves the loops and count-to-infinity problems by using incremented sequence number for each destination. It is one of the earliest protocols proposed to be a suitable candidate for ad hoc networks. The path to a destination is selected using the distance vector shortest path routing algorithm. As it is a table-driven routing protocol, the routing table maintained at every node contains the shortest distance and the first node on the path to every other node in the network. In order to keep the routing information and network topology up to date, the routing tables are exchanged between neighbours in regular intervals. In addition, when the node notices a significant change in the local topology since the last full table updating, the node forwards the table. Therefore, any required route by any node to any destination is continuously available at all times. This exchange in routing tables introduce a large amount of control overhead to the network, hence, two types of update packets are used to update the routing tables in order to reduce the control overhead disseminated through the network:

- "Full dump" update packets: The full dump packets are used if significant changes are observed in the local topology or if more data packets need to be carried in an incremental update. Hence, this type of update packet carries all the available routing information.
- "Incremental" update packets: the incremental update packet is utilised when there are no significant changes in the local topology. This packet contains only the information altered since the last full dump occurred. The incremental update messages are propagated more frequently than the full dump packets.

The sequence number is used by the destination node to initiate a table update. For a particular destination node, the sequence number is always greater than the previous one. Depending on the sequence number of the table update, the node may either forward or deny the table. When the node receives an updated table, it has two choices for updating its routing tables: either update its routing tables based on the fresh received information or keep it for some time to select the best metric from the multiple update table received from different neighbouring nodes.

Route maintenance of a broken link in DSDV is handled by initiating a table update message by the end node of the broken link. This message assigns the broken link's weight to infinity and a sequence number greater than the one is stored for that destination. Each node that receives an updated table on infinite weighting entry will send the table to its neighbours in order to propagate the broken link information to the whole network. In this way, when a single link breaks occurs, the propagation of table update information is flooded to the whole network.

Analysis and discussion: As a result, it can be said that in DSDV, the routes to any destination in the network are available all times. On the other hand, the updates are propagated throughout the networks in order to maintain an up-to-date view of the network topology at all the nodes. This still introduces large amounts of overhead to the network due to the requirement of the periodic update messages (the interval time is in seconds). The overhead complexity is proportional to the number of nodes by the order $O(N^2)$, where *'N'* is the number of nodes in the entire network. This complexity is reflected on the scalability of the network. Therefore, the protocol is effective for creating ad hoc networks of small size. However, it is not scalable for a large ad hoc network since a large portion of the network bandwidth is used in the updating procedures and topologies are highly dynamic. A long amount of time in DSDV protocol is spent on generating and updating the routing tables. DSDV also has potential problems in high mobility rate of the nodes in the networks due to the instability of the network for a period of time before the update packets reach all the nodes in the network.

2.1.1.1.2 Fisheye State Routing (FSR)

Fisheye State Routing (FSR) [33, 34] protocol is an improvement of Global State Routing (GSR) [36] where both are based on the link state protocol. The update messages in GSR consume a considerable amount of network bandwidth due to the periodic transmission and the large size of the update message. In GSR, each node maintains four tables: a

Neighbour list, a Topology table, a Next Hop table and a Distance table. The FSR algorithm reduces the routing update overhead in large networks by introducing the notion of multi-level scope that is explained in the following section.

FSR utilises the fisheye technique to reduce routing overhead. The basic principle behind this technique is that the eye of the fish can capture with high detail the pixel information near its eye's focal point. This accuracy decreases as the distance from the centre of the focal point increases. This principle is implemented in routing in ad hoc networks by FSR in such a way that every node keeps accurate information about nodes in its local topology. The accuracy of the network information decreases with increasing the distance. The fisheye scope of the node is the set of nodes in the network that are within a given number of hops. Setting a different number of hops (multi-level of scope) will cover the entire network.

In comparison with GSR, reducing the size of the update message in FSR comes from the fact that, every update message does not contain information about all nodes in the network. Instead, it contains information about only the nodes within the scope that the update message is intended to reach. State updates corresponding to far away destinations (far scope) are propagated with lower frequency than those for close by destinations. However, the fisheye scope technique allows the exchange of update messages at different intervals for nodes within different fisheye scope distance, leading to a reduction of the update message size. By fisheye scope, the nodes in the centre scope have most up-to-date information. The accuracy of information decreases as the distance from the node increases. This procedure of dividing the network into different scope levels is done at each node, meaning that it is independent on a central entity.

Discussion: it can be concluded that since FSR significantly reduces the bandwidth consumed by link state update messages in comparison with other link state routing protocols, FSR enhances the scalability of relatively large mobile ad hoc networks. In spite of easily locating destinations due to the flat addressing scheme and the availability of topology map, the size of the routing table and processing overhead limits its scalability. The main disadvantage points of FSR are the routing table storage complexity and the processing overhead.

2.1.1.1.3 Wireless routing protocol (WRP)

The Wireless Routing Protocol (WRP) [30] ensures fast convergence and freedom of count-to-infinity problem by using the predecessor information (readily available routing information). In order to maintain an up-to-date view of the entire network and routing information among all nodes, every node has to have a readily available route to every destination node in the network. This requires each node to maintain four routing tables: Distance table, Routing table, Link-cost table, and a Message Retransmission List (MRL) table. The distance table contains information about the neighbours of a node, where each entry contains the distance and the penultimate node received by a neighbour for a specific destination. The routing table keeps the shortest distance, the predecessor node and the next node to destinations as well as a flag indicating the status of the route. The link-cost table contains the cost of relaying messages through each link and the number of update periods passed since the last successful update was received from that link. Each entry of the MRL is for an update message that is to be retransmitted. This entry contains the sequence number of the update message, a retransmission counter and a list of updates sent in the update message. The update message is deleted when the retransmission counter reaches zero after the entries in the update message for which no acknowledgment have been received are to be retransmitted.

Update messages between neighbouring nodes are used to inform each other of link changes or link breaks. This message contains a list of updates: the destination, the distance to the destination, the predecessor of the destination and a list of responses indicating which mobiles should acknowledge (ACK) the update. After receiving the update message, all affected nodes modify their distance table entries to the corresponding nodes and check for new possible paths through other nodes.

Discussion: According to the above description of the main idea of WRP protocol, part of the novelty of WRP comes from the way in which it deals with the temporary routing loop and count-to-infinity freedoms. It avoids these problems by performing consistency checks of predecessor information reported by all the neighbours of a node. This gets rid of looping situations and involves fewer table updates when a link failure event occurs. However, the complexity of maintaining four routing tables at each node demands a larger memory overhead and greater processing power from each node as the size of the network increases. WRP is not suitable for higher dynamics and for very large ad hoc networks due to the increased amount of the control overhead involved in updating table entries at high mobility.

2.1.1.1.4 Cluster-head Gateway Switch Routing (CGSR)

Unlike other table-driven routing approaches that are based on flat topologies, the Cluster-head Gateway Switch Routing (CGSR) [37] uses a hierarchical network topology and uses DSDV as an underlying protocol. CGSR gathers nodes into clusters and in each cluster, a special node named a "cluster-head" is elected dynamically by using a distributed algorithm called Least Cluster Change (LCC) [37]. In this algorithm, a cluster-head change occurs in one of two cases. The first case is when two cluster-heads come into one cluster. This will lead to a situation where someone has to give up its cluster-head position by using lowest-id or highest-connectivity. The second case occurs when one of the nodes moves out of range of all cluster-heads. All nodes in the communication range (within a single hop) of the cluster-head belong to its cluster as member nodes. The cluster-head keeps track of the nodes in its own cluster and of the cluster-heads in the other clusters.

In CGSR, all communications passes through the cluster-head. Communication between cluster-heads takes place through nodes that are in the communication range of two or more cluster-heads. These nodes are called gateway nodes from one cluster to another (members of more than one cluster). Therefore, transmitting data packets takes place through cluster-heads and gateways in such way: Cluster-head⇨Gateway⇨Cluster-head⇨Gateway⇨and so on.

In CGSR, each node maintains two tables; one is a cluster member table containing the destination cluster-head for every node in the network; and one is a distance vector (DV) routing table that keeps the list of next-hop nodes for reaching every destination cluster. The cluster-head node broadcasts cluster member table periodically and each node on receiving this table updates its own table. If a node has a data packet to be routed, it finds the nearest cluster-head to the destination depending on the cluster member table and the routing table. Then it will get the next hop to reach the cluster-head selected above from its routing table and transmits the packet to that node.

By clustering, an effective allocation of wireless channels among different clusters is possible which, therefore, enhances spatial reuse amongst clusters. For example, different cluster-heads could use different spreading codes on a CDMA system. Whilst within a cluster, a token approach is used for sharing the bandwidth among the members and for giving priority to cluster-heads to maximise channel utilization and minimise delay.

Discussion: Grouping nodes into clusters reduces the routing table size by keeping one entry for one whole destination cluster. CGSR provides better bandwidth utilization and facilitates the priority scheduling schemes with token scheduling and gateway code scheduling. This is because CGSR depends on clustering nodes, and communications go through the cluster-heads. On the other hand, this way of clustering degrades the performance of this routing protocol, because CGSR increases the path length and instability in the network at high mobility when the rate of change of cluster-heads is high. In addition, the selection of the cluster-heads causes complexity and overhead due to the difficulty in maintaining the cluster structure in a mobile environment all the time.

Another matter of concern is the power consumption at the cluster-head nodes due to the heavy tasks assigned to these nodes (e.g. higher computation and communication load than other nodes). This will conduct to frequent changes in the cluster-head and single point failures at the cluster-heads and gateways. Hence, this leads to multiple route breaks. All these would reduce the scalability of the network, which is extremely undesirable.

2.1.1.2 Reactive Routing Protocols

Numerous protocols of this type have been proposed. The most typical reactive routing protocols are the Dynamic Source Routing (DSR) [13, 38], Ad hoc On-demand Distance Vector (AODV) [11], Temporarily Ordered Routing Algorithm (TORA) [39, 40], Associativity-Based Routing (ABR) [10, 41], and Signal Stability-Based Adaptive (SSA) routing [9].

This category of routing protocols is also called on-demand routing protocols that are proposed only for ad hoc networks. The work in this thesis falls into this category. The main characteristic of mobile ad hoc networks is the dynamic topology; hence, in order to follow the topology changes, frequent updates of the global topology information is required at each node. This, however, consumes considerable bandwidth. To further complicate things, sometimes the received routing information updates may expire before this information is needed. In this case, the routing information becomes a waste of bandwidth as it is obsolete. To reduce the unnecessary routing information updates and the consumed amount of bandwidth, the concept of reactive or on-demand routing protocol has been proposed by Johnson [42].

On-demand routing protocols [43], unlike proactive routing protocols, do not maintain the network topology information and route to each destination of the network. Instead, they establish the necessary routes when required (on demand) by the source, by using a route discovery process. Generally, when a route is needed by a source *S*, a Route Request (*RREQ*) packet is triggered and floods it into the network to construct a route to the required destination, *D*. When *D* receives the *RREQ*, a Route Reply (*RREP*) packet is then sent back by *D* to *S*. *RREP* is sent using link reversal if the route request has travelled through bi-directional links, or by piggybacking the route in a route reply packet via flooding. In on-demand routing protocols, the main functions of routing algorithm are route discovery and route maintenance.

1) **Route discovery:** In the MANET, as already mentioned earlier, the route discovery is triggered by flooding *RREQ* through the network in a controlled manner, seeking a route to the destination. Firstly, the source consults its current routing table about a valid route towards the destination that is already established. If there is no valid route, it broadcasts a route discovery packet that is re-broadcasted by intermediate nodes until it reaches the destination. Intermediate nodes that receive the route discovery packet forward the discovery packet and may create some data structures to identify the route. The destination then answers by returning a *RREP* packet to the source. Many optimizations to this basic route discovery mechanism are proposed in order to limit the frequency and spread of route discovery attempts.

2) **Route maintenance:** During transmission of a packet in the network, route maintenance is used to detect if the network topology has changed such that the route followed by this packet has broken. The link breaks could result from node mobility, the node shutting down due to power draining, fading environment, signal interference, high error rate or packet collisions. A node detects a link break and loses communication to the next node when it receives a link layer feedback signal from the MAC protocol, or it does not receive passive acknowledgments (MAC protocols such as MACAW and IEEE 802.11 [44] have this capability). Most wireless MAC protocols, such as IEEE 802.11 [44], keep retransmitting each packet until a link-layer acknowledgment is received, or it reaches the maximum number allowed for transmission attempts. Each node along the route is responsible for detecting the broken link to the next hop. If a link failure is found along the path by a node; either the node notifies the source that may then decide to initial new route discovery process to find a new route, or a local repair is launched by the node that discover the broken link to bypass the broken link.

According to the route information carried in data packets, the reactive routing protocols can be categorised into two groups: source routing (Full path) and hop-by-hop routing (point-to-point routing) [45]. In source routing protocols such as the Dynamic Source Routing protocol (DSR) [38] and the Associativity-Based Routing Protocol (ABR) [10, 41], the complete route address from the source to the destination nodes is carried by each data packets. Hence, the data packet is forwarded toward the destination along the path mentioned in the header of this packet. An advantage arises as a result of using source routing type. At intermediate nodes, there is no need to maintain neighbour connectivity and routing information for each active route for forwarding the packet towards the destination.

In point-to-point routing approaches such as the AODV protocol [11], the data packet only maintains the destination and next hop addresses. The intermediate nodes along the path maintain routing tables, which are used for forwarding the packet towards the destination. Using routing tables at each node in the network gives an advantage to hop-by-hop routing in that by dynamically updating the topology changes of MANETs when nodes receive fresher topology information, they will forward the data packets over fresher routes.

Discussion:

In on-demand routing protocols, compared to proactive routing protocols, control traffic overhead is greatly reduced. However, the reactive source routing protocols do not scale well in large networks since the number of nodes contributing to each route will become larger. This results in an increase in the potential route failure and an increase in the amount of overhead carried in each header of each data packet. The main two drawbacks in hop-by-hop routing are that each node may require an awareness of its neighbours through exchanging beaconing messages and each intermediate node should maintain routing information for each active route to other destinations. Because of this, a number of different reactive routing protocols have been proposed to increase the performance of this kind of protocol [9-11, 13, 38, 39 and 40]. In general, reactive routing protocols are more common than proactive and hybrid protocols due to the low routing overheads and limitation in hardware capabilities of handheld devices used in ad hoc wireless networks in terms of communication, storage and power. These grant reactive routing protocols to be ideal for most ad hoc networks applications.

2.1.1.2.1 Ad hoc On-demand Distance Vector

The AODV routing protocol [11] is a reactive routing algorithm falling into the hop-by-hop routing group. The sequence numbers are used by AODV to ensure maintenance of the freshness of routes and utilisation of the most recent routing information.

What is different about the AODV over the generic on-demand system is the use of the sequence number of the source and the destination in addition to flooding the route request packet across the network in order to find the route to the intended destination. The RREQ packet includes the source node's IP address, the destination node's IP address, the current sequence number of the source, the broadcast ID, the most obtained sequence number for the destination and the time to live (TTL) field.

In AODV, the validity of a route at the intermediate node is decided by the corresponding destination sequence number greater than or equal to that contained in the RREQ. The node that wants to send RREP places the current sequence number of the destination, as well as its distance in hops to the destination, into the RREP. Then a RREP is unicasted back to the source along the path followed by RREQ. Once the source node receives the RREP packet, it starts transmitting data packets to the destination. In case the route discovery timer expires and the source node does not receive a RREP, it rebroadcasts the RREQ. This discovery attempt is repeated up to some predetermined maximum number of times. If no route is discovered (no route reply is received) after the maximum number of attempts, the session is aborted.

If a link break occurs while the route is active and any neighbour of the upstream node uses that link, the node creates and propagates a Route Error (RERR) packet to the source node to inform it of the now unreachable destinations. The RERR packet contains all IP addresses of unreachable destination nodes due to the link break and their sequence numbers are incremented by one. The node then broadcasts the packet and invalidates those routes in its route table. After receiving the RERR, if the source node still needs the route, it can reinitiate route discovery.

Discussion: the main advantage of this protocol is that it uses the on demand approach for establishing the routes. On the other hand, the serious drawbacks of this protocol are the multiple RREP packets generated in response to a single RREQ packet. This can lead to heavy control overhead added to the already heavy control overhead occurring due to the flooding the RREQ packet across the network. This overhead is very costly and results in serious redundancy, contention and collision. Therefore, one of the aims in this research is to reduce the overhead in on demand routing protocols.

During the route discovery, an RREQ packet is sent out to all neighbours. Each neighbour in turn forwards it to its neighbours, without taking into account if the neighbour is about to be out of the coverage range or not. In time, this could fail to send the data along discovered route due to the link break occurring by one neighbour moving outside the range of the previous node in the path.

2.1.1.2.2 Dynamic Source Routing Protocol

The Dynamic Source Routing protocol (DSR) [13, 38] was developed at Carnegie Mellon University. It is a direct descendant of the source routing scheme. It uses source routing instead of hop-by-hop packet routing. It is designed specifically for use in multi-hop wireless ad hoc networks. DSR limits the bandwidth used by control packets needed for establishing routes by eliminating the periodic table-update messages. These messages are required by a node in the reactive approach to inform its neighbours of its presence.

The difference between DSR and AODV is that DSR includes the full path between the source and destination nodes in the reply message. In addition, each node visited by the RREQ packet includes its address in this packet before broadcasting it across the network. Each node receives a route request packet, retransmits the packet to its neighbours in two cases. 1) It is the first time the node receives the packet and has not already forwarded it. 2) The node is not the destination node. The destination node, on receiving a route request packet, sends a route reply back to the source. The route reply packet carries the route traversed by the route request packet received.

The use of source routing and the sequence number of the packet has three advantages:

1) It prevents loop formation.
2) It avoids the need for up-to-date routing information in the intermediate nodes through which packets are forwarded.
3) It avoids multiple transmissions of the same route request by an intermediate node that receives it through multiple paths.

If the nodes are operated in the promiscuous mode (the mode of operation in which a node can receive the packets that are neither broadcast nor addressed to itself), they can also learn about the neighbouring routes traversed by data packets.

Several optimisation techniques have been incorporated into the basic DSR protocol to improve the performance of the protocol. For example, utilisation of the route cache information at intermediate nodes to reply to the source, when they receive a route request packet. In this case, the intermediate nodes should have a route to the corresponding destination. Another optimization is to eliminate the route acquisition latency by piggybacking data on route request packets.

Discussion: Eliminating the need to periodically flood the network with update messages and establishing a route only when it is required (on-demand) are the major advantages for this protocol. On the other hand, DSR does not locally repair a broken link during the route maintenance mechanism. Instead, when a link break occurs, a Route Error (RERR) packet is sent to the original sender to invoke a new route discovery phase. Nodes that receive a route error message delete any route entry from their route cache, which uses the broken link. Since the packet carries the full path to the destination in its header, DSR dose not scale well in large networks. DSR performs well only in static and low mobility environments while the performance degrades rapidly with increasing mobility. In spite of finding the route on demand, a considerable routing overhead is involved (it is directly proportional to the path length) due to the source-routing mechanism employed in DSR in flooding RREQ. The DSR establishment mechanism yields a long delay when a packet needs to go through a new link. In the proposed mechanisms, which are on-demand techniques, the effect of the mobility of nodes is reduced by exploiting one of the positive aspects of mobility, which is the heading direction. In the same time elongating the lifetime of the link, in order to produce a more adaptive mechanism with mobility and in order to reduce the overhead caused by flooding the route request packets in the network.

2.1.1.2.3 Associativity-Based Routing Protocol

Associativity-Based Routing Protocol (ABR) [10, 41] is a different approach to mobile routing. It is a beacon-based, on-demand routing protocol invented by Toh [41] and developed at Cambridge University. ABR is a distributed routing protocol designed for mobile ad hoc networks. Routes in ABR are selected based on the wireless link stability. The link is considered stable or unstable based on its temporal stability. This is determined by counting the periodic beacons between the neighbour nodes. Since the ABR protocol is beacon-based, each node produces periodic "hello" messages to represent its existence to its neighbours. These beacons are used to update the associativity table of each node where each node maintains the count of its neighbours' beacons. With the temporal stability and the associativity table, the nodes are able to classify each neighbour link as stable or unstable based on the beacon count corresponding to the neighbour node concerned. The link corresponding to a stable neighbour is termed as a stable link. There is no need for periodic route updates because ABR is a source routing protocol.

The source node triggers the route discovery by flooding the network with route request packets if the route to the destination is not available in the cache. These packets are forwarded only once by the intermediate node that received the route request packet. The intermediate node appends its address and its associativity ticks (the beacon count) to the packet. When the route request packet reaches the destination, the destination waits a period, $T_{RouteSelectTime}$, before selecting the route that has the maximum proportion of stable links. If multiple routes have the same overall degree of stability, the shorter of them will be selected. Once the route has been chosen, the destination sends a Reply packet back to the source along the same path.

If a link break is noticed at an intermediate node (the broken link is detected through the beacons), the uplink node closer to the source initiates a local route repair process by broadcasting a route repair packet with limited TTL (time to live). If this node fails to repair the broken link, the next node in direction to the source (the uplink node) reinitiates the local query broadcast. This process continues until the node in the middle of the broken path fails to repair the dead link. After that, the source is informed, which initiates a new route establishment phase.

Discussion: In ABR, stable routes have a higher preference compared to shorter routes, which results in fewer path breaks. However, sometimes, the chosen path may be longer than the shortest path because of the preference given to stable paths. Local query broadcasts may result in high delays during the route repair. In addition, consider that two neighbour nodes are moving in the opposite direction of each other. Each node receives the required threshold number of beacons from the other node, which allow each node to consider the other node as preferable neighbour node. After selecting the path and receiving a route reply from the destination, the link between these two nodes is broken due to then being in opposite directions to each other. The broken link is a result of moving out of the transmission range of each other. This will lead to route unavailability. As a result, it is wise to consider the mobility aspect as an important metric in selecting the preferred neighbour. This is the core work in this thesis.

2.1.1.2.4 Signal Stability-Based Adaptive Routing Protocol

The Signal Stability-Based Adaptive Routing protocol (SSR) presented by Dube et al. [9], unlike the algorithms described so far, selects routes based on the signal strength between nodes and a node's location stability. The location stability defines paths, which have existed for a longer period than other paths. Therefore, SSA needs beacon messages between nodes (beacon-based like ABR) in which the signal strength of the beacon is measured for determining link stability. This technique of route selection requires that

SSR uses an extended radio interface to measure the signal strength from beacons. A link is classified as stable or unstable according to the received signal strength.

SSR consists of two cooperative protocols: the Forwarding Protocol (FP) and the Dynamic Routing Protocol (DRP). FP performs the routing to forward a packet to the destination. DRP receives and processes all transmissions, maintains the routing table and the Signal Stability Table (SST). SST contains the beacon count and the signal strength of each of its neighbouring nodes. This table is used to forward the route request over strong links for finding the most stable end-to-end path. A node considers a link as strong and stable if the node has received strong beacons for the past few beacons.

If the destination is not found in the routing table, FP triggers a route request packet to find a route. The most important task in route finding is that route request packets are forwarded to the next hop only if they are received over strong channels and have not been previously processed. The packets received over a weak link are silently dropped without being processed. If the stable link is not available to forward a route request to a destination, FP floods the route request throughout the network without considering the stability of links as the forwarding criterion. The destination chooses the first received route request packet and initiates a route reply packet to send back to the source. The DRP of the nodes along the path update their routing tables accordingly. The route request packets that reach the destination traverse on the path of strongest signal stability.

Discussion: The main advantage of SSA is that this protocol forwards packets to a destination along stable routes based on the signal strength between nodes. On the other hand, as in the ABR routing protocol, consider two neighbour nodes that are moving in the opposite direction of each other. Each neighbour receives the required number of strong beacon signals from the other neighbour, which let each node consider the link to the other node as a strong/stable link. As they are moving outside the transmission range of each other, the link between these two nodes is going to be quickly broken in spite of receiving a strong signal from each other. This will lead to route unavailability after the link break. As a result, it is, again, wise to consider the mobility aspect as an additional important metric added to signal strength criterion for establishing the path by implementing one of the techniques proposed in this thesis.

The technique of route selection requires that SSR uses an extended radio interface to measure the signal strength from beacons. Due to the rapid development in the technology such kind of interfaces are easily integrated in most devices.

One further disadvantage of SSA is that if the stable links are not available to forward a route request to a destination, the node floods the route request throughout the network without considering the stability of links as the forwarding criterion. The route request packets received over weak links are not considered but dropped without being processed. In this case, if there is no stable link and there are some other links with different weakness levels, no one of these links is taken, in spite of that maybe one of these weak links is going to be strong after short time. Hence, RREQ is going to be dropped without selecting the strongest link between the weak links. For example, one node just entering the transmission range of other stationary node, and moving toward the location of the stationary node.

Another disadvantage of SSA is that broken links are locally detected but not repaired. Instead, when a node detects a link break, the node sends an error message to the source indicating which link has failed. When the source receives the error message, it sends an erase message to notify all nodes of the broken link and initiates a new route request process to find a new path to the destination. This leads to multiple flooding of route request messages that restricts the bandwidth.

2.1.1.3 Hybrid Routing Protocols

The hybrid routing protocols are a class that offers routing solutions that are both reactive and proactive. They increase the network scalability by allowing close nodes to form a near zone and determining routes to far away nodes using a reactive strategy. The close nodes work together to reduce the route discovery overheads by proactively maintaining routes to nearby nodes.

Most hybrid protocols proposed to date are zone-based, which means that the network is partitioned or seen as a number of zones by each node. In protocols belonging to this category, each given node partitions the area of the network into two distinguished regions. The nodes in near distance from the node, or inside a particular geographical region, are forming the routing zone of the given node. In the routing zone, a proactive (table-driven) approach is used. An on-demand routing approach is used for nodes located in the area beyond the routing zone. The most typical hybrid routing protocols are Zone Routing Protocol (ZRP) [46], and Core Extraction Distributed Ad hoc Routing (CEDAR) algorithm [47]. The latter selects a minimum set of nodes as a core to perform QoS route computations.

2.1.1.3.1 Zone Routing Protocol (ZRP)

ZRP [46] is a hybrid routing protocol that incorporates the merits of both on-demand and proactive routing protocols. That is, ZRP divides its network in different zones according to the nodes local neighbourhood. Each node has its own zones since each node has an intra-zone and an inter-zone. The intra-zone is a limited zone in the k-hop neighbourhood of the node, while the inter-zone is the zone beyond the intra-zone. The intra-zone is referred to as a routing zone. Therefore, each node in the network may be within multiple overlapping zones, and each zone may be of a different size. The size of a zone is given by a radius of length, where the number of hops is the outer boundary of the zone. For every node, the peripheral nodes are the nodes whose minimum distance to the node in question is equal to the zone radius. ZRP is similar to a cluster in terms of dividing the network area into a number of zones. This is with the exception that in ZRP, every node acts as a cluster head and a member of other clusters.

For nodes within the routing zone of a node, this node uses proactive routing protocols to maintain routing information. For those nodes outside of the routing zone, on-demand routing strategy is adopted when inter-zone connections are required. In routing zone, the Intrazone Routing Protocol (IARP) proactively maintains routes to destinations. IARP can be any proactive routing depending on the implementation. In order to find a route to

a destination node outside the routing zone, reactive IntErzone Routing Protocol (IERP) is performed. IERP uses an on-demand routing approach. This approach uses route request query (RREQ) and route reply (RREP) packets to discover a route.
When a node requires a route to a destination and the intended destination is not in the routing table of IARP, ZRP considers that the destination node must be outside of its routing zone. Thus, a RREQ packet is broadcast to the peripheral nodes. This type of broadcasting is called Bordercast Resolution Protocol (BRP). The broadcasting of RREQ continues from one node's peripheral nodes to other peripheral nodes until reaching a node that the destination is within its zone.

Discussion: Since ZRP is a hybrid routing protocol that uses both reactive and proactive schemes [48, 49] it exhibits better performance. That is, ZRP protocol limits the periodic flooding (proactive overhead) to only the nodes within the routing zone. It also restricts the on-demand route discovery (search overhead) to only selected peripheral nodes. Nevertheless, potential inefficiency may occur when the RREQ packet is flooded across the entire network. In addition, due to the use of hierarchical routing of establishing the path to a destination, this path may be suboptimal. Increasing the size of routing zone requires each node to have higher-level topological information and a greater memory requirement.

2.1.2 Location-Based Routing Protocols

The Mobile Ad-hoc Networks [50] working group within the Internet Engineering Task Force (IETF) has proposed many existing unicast routing protocols such as AODV [11], DSR [38], DSDV [29], WRP [30], FSR [33, 34], Optimised Link State Routing Protocol (OLSR) [32], Landmark Routing Protocol (LANDMAR) [51], Temporally-Ordered Routing Algorithm (TORA) [39, 40] and Cluster Based Routing Protocol (CBRP) [52]. These protocols lean on the state of all links between nodes in the network or only links between nodes forming a route from a source to a destination. These kind of protocols may not perform well (scale) in larger mobile ad hoc networks. With the advent of GPS [53- 55], there has been a growing focus on another new class of routing algorithms that make use of node location information while building routes. These algorithms improve the efficiency of routing and increase the network scalability by reducing the total routing overhead. Such kind of routing protocols that require GPS are Location-Aided Routing (LAR) [1, 14], Distance Routing Effect Algorithm for Mobility (DREAM) [25], Zone-Based Hierarchical Link State (ZHLS) [15], Flow Oriented Routing Protocol (FORP) [16], Grid Location Service (GLS) [56], and Greedy Perimeter Stateless Routing (GPSR) [17, 18].

The general ideas behind designing these routing protocols are either to reduce the propagation of control messages as in LAR, or to control the packet flooding as in DREAM, or to reduce intermediate system functions, or to make simplified packet forwarding decisions as in GPSR.

A routing protocol that relies on geographical information (for example GPS information) [1, 14-18, 25, 56] may not work well in certain situations where such information is not available or accessible. For example, if the node is underground, inside a building or in extreme terrains, it may not be possible to use such routing protocols [21, 22]. Hence, an alternative source of information has to be available to let the routing protocol do its job properly. For example, a digital compass that delivers the direction of nodes, which is utilised in the proposed schemes to determine the heading direction angles of the nodes. Table 2-1 shows the performance comparison between the protocols

Table 2-1: Performance comparison between protocols

	Routing technique	**Source route**	**Neighbour detection**	**Loop freedom maintenance**	**Multiple paths**	**Communication Overhead**
AODV	Reactive/ Flooding	No	HELLO message	Sequence number	No	High
DSR	Reactive/ Flooding	Yes	No	Source route	Yes	High
DSDV	Proactive/ Flooding	No	HELLO message	Sequence number	Yes	High
FSR	Link state update	No	Periodical link state updates	Limited scope (multi-level	No	reduces the routing update

				scope		overhead in large networks
WRP	Proactive	No	HELLO message	sequence number and checks of predecessor information	Yes	High
CGSR	Proactive	No	broadcasts cluster member table periodically	Limited scope of transmission to a cluster	No	the selection of the cluster-heads causes overhead
ABR	Reactive / based on the wireless link stability	No	periodic beacons between the neighbour nodes	sequence number	No	Low
SSR	Reactive / based on the signal strength	No	beacon messages between nodes	sequence number	No	Low
ZRP	Hybrid	No	Hello message in the Intrazone	sequence number	Yes	Low in outer zone

2.2 Mobility in Ad Hoc Wireless Networks

Routing protocols for wired network cannot be utilised in ad hoc wireless networks where frequently changing the network topologies due to nodes mobility. Therefore, when designing a routing protocol for mobile ad hoc wireless networks, the protocol must be able to perform efficient and effective mobility management. This protocol should also be able to reduce the effect of mobility of nodes that affects the overall performance of the network.

The significant effect of mobility in ad hoc networks is the increased rate of links failure and hence the activation of these broken links when the mobility of nodes is increased. This increases both the congestion due to traffic backlogs and the volume of control traffic required to maintain routes. Thus in order to achieve adaptive routing responsiveness and efficiency, the ultimate protocol design goal has to be the diminution of reaction to mobility [6]. Some of the work on routing has been done in the context of reducing the effect of mobility on the performance of routing protocols [2, 7-11]. These protocols differ in the approach used for searching a new route and/or modifying a known route, when hosts move.

In mobility-aware clustering [6, 57], the mobility behaviour of mobile nodes is the main influencing factor taken into consideration. A number of routing approaches based on clustering are proposed [58-62]. The benefit of dividing ad hoc network into clusters is that it reduces the effects of mobility. This reduction is achieved by allowing only some selected nodes from all the nodes in the network to take the responsibility of establishing the route to a destination. The set of *cluster heads* and *cluster gateways* can normally form a virtual backbone for inter-cluster routing. Thus, the generation and spreading of routing information can be restricted in this set of nodes.

However, a cluster-based MANET has its drawbacks. In comparison with a flat-based MANET, additional cost is required for constructing and maintaining the structure of network cluster. In a dynamically changing scenario, explicit message exchange between mobile nodes is required to maintain a cluster structure. The higher computation and communication load needed at cluster heads and gateway nodes than other nodes affect the reliability of network in the event of failure of any of these nodes. An additional side effect of cluster-based routing protocols is *the ripple effect of re-clustering.* This again is caused due to the mobility of nodes, or sleeping a node, or draining the power from the battery of a mobile node. This side effect often results in reselecting some cluster head and [63], may affect the structure of many clusters that may greatly affect the performance of upper-layer protocols.

Backbone-based routing protocols select a small subset of the network nodes based on its status and organise the selected node to form a backbone. The backbone is guaranteed to be connected if the original network is connected. The key feature in the backbone-based approach is the broadcast mechanism used to replace the flooding mechanism used by most on-demand routing protocols. This is performed by a unicast mechanism that restricts the unicast of route request packets to selected core nodes and a subset of non-core nodes. This approach provides explicit mechanisms to handle the mobility of the nodes [7, 64- 67]. Kozat et al. [65] determined the properties of selecting the backbone nodes. They showed that the backbone (core nodes) should satisfy the two properties of *a minimum connected dominating set (MCDS)*, to ensure a reliable broadcasting in an ad hoc environment. These properties are: *i)* any node in the network either is a backbone node or is a neighbour of a backbone node, *ii)* the backbone nodes are connected to each other via other backbone nodes.

The main drawbacks of this type of protocol are the heavy route computation carried out at the core nodes and the movement of the core nodes that affects the performance of these protocols. In addition, a significant amount of control overhead occurs due to the core node update information.

Researchers have written several papers on analyzing and proposing models to study the effects of mobility. Mikko [68] presented a model that allows describing relative difficulty of different mobility models for ad hoc networking. He also proposed that the route lifetime can be used as an indicator of the effects of mobility for reactive ad hoc routing. Different studies are introduced and tended to measuring the effects of mobility. Larsson and Hedman [69] proposed a model to calculate a mobility metric called *mobility, M.* This metric is used to describe the difficulties for routing in ad hoc, due to the mobility of nodes. As described by Larsson and Hedman [69], the mobility metric, M_x, of node x measures the change in average distance, A_x from one node, x, to all other nodes, n, between successive simulation time steps Δt. If T is the whole simulation time and n is the number of all nodes, then the average mobility for a node x through the time T is given by:

$$M_x = \frac{\sum_{t=0}^{T-\Delta t} |(A_x(t) - A_x(t+\Delta t))|}{T - \Delta t} \qquad (1)$$

Then, the average mobility for the whole scenario is:

$$M_{Avg} = \frac{\sum_{i=1}^{n} M_i}{n} \qquad (2)$$

Johansson et al [70] proposed a model to calculate mobility metric depending on the relative velocity between nodes. They defined the mobility measure, M_{xy}, between two nodes x and y as the absolute relative speed between these two nodes taken as an average over the simulation time T. The mobility metric formula is given by:

$$M_{xy} = \frac{1}{T} \int_0^T | v(x, y, t) | \, dt \qquad (3)$$

The total mobility metric over all node pairs M for a scenario is given by the following definition:

$$M = \frac{1}{|x, y|} \sum_{x,y} M_{xy} \qquad (4)$$

where $|x, y|$ is the number of distinct node pairs (x, y).

Turgut et al [71] investigated the expected lifetime of a route and concluded that the expected lifetime of the route is the important metric to be taken into account in routing. Choudhury and Vaidya [72, 73] evaluate the performance of a reactive routing protocol for different scenarios using directional antennas in order to reduce the effect of node movement. They proposed routing strategies that adapt the routing protocol to directional communication. The outcome of their result is that by using directional antennas, ad hoc networks may achieve better performance, and scenarios exist in which using omnidirectional antennas may be more appropriate. The drawback of using directional antennas is in its hardware where multiple antennas are used, and the need to control the switching between these antennas.

As discussed above, the mobility is a very important factor that concerns most researchers who try to find a way to get rid of the side effects caused by mobility on the functionality of the network. In addition, different models are proposed for measuring the effect of mobility on the functionality of routing protocols in ad hoc wireless networks. These models rely on a single mobility metric, which quantifies the effects of mobility.

2.2.1 Mobility Models

Almost all work on mobile ad hoc networks relies on simulations, as simulations provide a valuable means to compare different protocols and study their performance in terms of efficiency and robustness. Consequently, when simulating a protocol for a mobile ad hoc network, it is necessary to use one of the available mobility models. This model accurately represents the mobile nodes and their movements in the network space where the nodes are supposed to be distributed. Only in this type of scenario, it is possible to determine whether or not the proposed protocol will be useful when implemented [74]. The mobility model plays an essential role especially in routing in mobile ad hoc networks. Traces and synthetic models are the two types of mobility models used in the simulation networks [75]. Trace mobility models are the mobility patterns that are monitored in real life. However, in the environments of mobile ad hoc networks, it is difficult to model the network if traces have not yet been created. Thus, it is necessary to use synthetic models that try to represent the behaviours of mobile nodes in a realistic manner without the use of traces.

Several mobility models have been presented in recent years [74-80]. Turgut et al. [71] presented four mobility models deterministic, partially deterministic, Brownian motion and Brownian motion with drift.

In **Deterministic Models,** the movements of all the nodes are completely defined. In **Partially deterministic model,** the directions of movement of all the nodes are known with a certain probability. It assumes that there is a probability distribution function for the direction of motion. In **Brownian motion model,** the direction of movement is a continuous random variable uniformly distributed between 0 and 2π. In addition, the velocity at any given time is random. In **Brownian motion with drift model,** the nodes move randomly, as in the previous model, but the probability cloud has a general direction of movement. Several mobility models have been described that represent mobile nodes whose movements are independent of each other (e.g., the Random Waypoint Mobility Model [74]). Different mobility models represent mobile nodes whose movements are dependent on each other (e.g., group mobility models). In general, the mobility models could be classified as Random-based models and Group-based models. Some of the random-based mobility models are [74]:

1) Random Walk Mobility Model.
2) Random Waypoint Mobility Model.
3) Random Direction Mobility Model.
4) A Boundless Simulation Area Mobility Model.
5) Gauss-Markov Mobility Model.
6) FreeWay Mobility Model

In an ad hoc network, however, there are many situations where mobile nodes move together or form groups (the heading direction angle of nodes in each group is nearly similar). For example, vehicles on a road or, in a military scenario, a group of soldiers searching a particular plot of land, all working together in a cooperative manner to accomplish a common goal. Some of proposed group-based mobility models are [74-78]:

1) Exponential Correlated Random Mobility Model.
2) Column Mobility Model.
3) Nomadic Community Mobility Model.
4) Pursue Mobility Model.
5) Reference Point Group Mobility Model.

2.2.2 Mobility Prediction

In terms of mobility prediction routing protocols, a number of prediction-based mobility schemes have been proposed for ad hoc networks [8, 81-84]. Samarth and Nahrstedt [84] present a location-delay prediction scheme, based on a location-resource update protocol, which assists a Quality of Service (QoS) routing protocol. This scheme used geometric coordinates, direction of motion, velocity and resource information pertaining to the node that is used in QoS routing. However, the updated protocol in this scheme involves flooding of location and resource information pertaining to a node to all the other nodes in the network. Such a full flooding of the network involves a considerable overhead due to the use of bandwidth. In addition, due to flooding, a huge number of duplicated packets are sent and frequent packet collisions take place in multiple access based MANET. On top of that, relying on many routing information sources (Location, speed, etc) which may not be always available to the network all at the same time, could affect the performance of the routing protocol. Su et al. [8] presented mobility predictions to enhance unicast and multicast routing protocols and utilises GPS location information [5]. The key idea in these mobility predictions is that during a live connection of the data packets each node that receives these packets will piggyback the position information of this node on these packets. This information is used to estimate the expiration time of the link between two adjacent nodes. Based on this prediction, routes are reconfigured before they disconnect. The main weakness of this scheme is that information about the position, the direction and the speed of each node should be provided to each node. The drawback of this scheme is that node movement is limited to some degree of regularity in the mobility pattern (non-random travelling pattern) with constant velocity. This is due to the assumption that nodes have simple mobility patterns without considering sudden change of direction. This means that the scheme cannot hold in some scenarios where the mobility prediction becomes inaccurate.

2.2.3 Summary of the Mobility

It is clear from the outcome of the above discussion that the mobility of nodes in MANET affects the lifetime of routes and becomes the concern of most researchers in mobile ad hoc networks. As a conclusion, there are two possible trends toward getting rid of the side effect of mobility in ad hoc networks: 1) most previous research has tended to alleviate the side effect of this mobility, without trying to get benefit from the mobility itself. 2) one good trend towards the mobility problem is to exploit the positive aspect of this phenomenon as much as possible, rather than finding a way to avoid the effects of this mobility.

2.3 Summary

Many types of routing protocols for mobile ad hoc networks are competing for different casting communication (unicast, multicast, multipath and broadcast communication). Despite this variation, it seems that one routing protocol cannot provide all the desired advantages and gives all the preferred functionality of routing. One protocol also cannot fit all the different scenarios and traffic patterns of ad hoc network applications that have been seen during the discussion of each routing protocol. This is due to the specific characteristics of mobile ad hoc network. These characteristics include mobility, power consumption, bandwidth-constrained and dynamic topologies. For instance, proactive/table-driven routing protocols are well suited for small scale, high mobility. They might not be considered an effective routing solution for mobile ad-hoc network. This is because nodes in such networks, in general, function with low battery power and with limited bandwidth. Therefore, in proactive routing protocols, in high mobility scenarios, each node will require large routing tables and more continuous updating of network topology changes. These result in consumption of bandwidth and battery life of the nodes and create unnecessary network control traffic overhead.

Reactive routing protocols are another example where one routing protocol cannot fit all the different scenarios and applications. These protocols perform well in a large-scale, but with low to moderate mobility scenarios. However, in general, reactive/on-demand routing protocols are more common because of their specific characteristics. Reactive routing protocols are ideal for applications when nodes in ad hoc networks are compact handheld devices, which are limited in storage, communication and power. The work in this thesis is based on an on-demand approach.

Maltz [85] illustrates the importance of on-demand routing protocols by saying: *"Efficient routing in an ad hoc network requires that the routing protocol operates in an on-demand fashion, and requires that the routing protocol limit the number of nodes that must be informed of topology changes. Ad hoc networks running such a protocol can be* *designed and implemented, and they perform well enough to support useful applications."*

In summary, routing is one of the important cores in mobile ad-hoc networks. Every routing protocol has its strengths and drawbacks and aims at a specific application. In addition, the strengths of a protocol could be drawbacks in another protocol. Current routing protocols provide routing solutions up to a certain level for certain scenarios. However, they are lacking the ability to handle other scenarios with related points (such as nodes mobility with long-lived routes to the destination). If these protocols could be extended further, or new routing protocols are designed by taking into account other routing related factors, it may come out with a standard routing solution for mobile ad-hoc networks.

Chapter 3
Heading Direction Routing Protocols and Modelling

3.1 Motivation

Several routing protocols have been proposed for ad hoc networks as a solution for mobility effects in multi hop communication. Many of these protocols utilise basic network services such as geographic messaging and flooding resource location. These lead to significant control overhead and interference to ongoing traffic, which are often unbearable. Flooding techniques may result in excessive redundancy, contention, and collision. This result is referred to the notorious broadcast storm problem [86].

In order to reduce the overhead and flooding effect, Kumar and Xue [87] introduce a scheme to reduce the flooding and overhead involved in the route discovery to the destination. This scheme utilises forwarding packets to certain nodes, which fall into a determined region. These nodes are selected based on the location of the final destination and the location of the intermediate node. However, this scheme did not take into account the lifetime of the link between neighbouring nodes for establishing long-lived routes.

The work carried out this thesis falls into on-demand routing protocols category. As mentioned in chapter 2, in AODV, the serious drawbacks are the multiple RREP packets generated in response to a single RREQ packet. This can lead to heavy control overhead added to the heavy control overhead occurring due to flooding the RREQ packet across the network. This overhead is very costly and results in serious redundancy, contention and collision. Therefore, one of the aims in the proposed approaches in this thesis is to reduce the overhead in on demand routing protocols.

DSR is an on-demand routing protocol. In spite of finding the route on demand, a considerable routing overhead is involved, which is directly proportional to the path length. In addition, DSR establishment mechanism yields a long delay when a packet needs to go through a new link when already available link is broken. In the proposed approaches, which are on-demand techniques, the effect of the mobility of nodes is reduced by exploiting one of the positive aspects of mobility, which is the heading direction. In the same time the lifetime of the link is elongated, in order to produce a more adaptive mechanism with mobility and in order to reduce the overhead caused by flooding the route request packets in the network.

3.2 Research Methodology

The adopted research methodology toward the research goal comprises of the following main steps/activities: (1) identification of problems (via intensive literature reviews), (2) concept presentation (3) concept development, (4) validation and evaluation, (5) reflection and feedback, and (6) documentation/reporting findings and identification of directions for future research and development. Note that, in practice, the process is inherently iterative.

The research study was initiated with a two-stage literature review consisting of state-of-the-art and in-depth reviews. The state-of-the-art review was conducted for the recognition of the up-to-date developments for mobile ad hoc networks. Since the work in this research is intended to design new routing approaches and to reduce the effect of mobility in ad hoc networks, the literature review is focused on the following areas: routing protocols and mechanisms for ad hoc networks, mobility behaviour and effects in ad hoc networks, and application spectrum of ad hoc networks.

The second stage of the literature review – in-depth review, was conducted for the identification of specific research problems/questions. It also served the purpose of identifying potential solutions for the identified/selected problems, which may have been researched previously (but have not been sufficiently/extensively researched). In this research, the focus has been on the flooding reduction in ad hoc networks, the route lifetime, and the reduction of mobility effects. Note that, this step has been conducted continuously and in parallel with the other steps (step 3 to 5), throughout the period of this research study. This was necessary to ensure that potential developments in related areas could be continuously fed back to the other activities throughout the research period.

During the second and third step – concept presentation and development, four conceptual approaches were formulated. The first three approaches were concentrating on reducing the effect of mobility in ad hoc network by using the positive aspect of this mobility, which is the heading direction angle. The fourth approach was designed to find solutions to the failures occurring in the static centric server in the location service routing protocols. In the fourth step – validation and evaluation, an intensive simulation and software implementation for all the proposed approaches were formulated. It involved deeply understanding the simulation tool and the programming languages by which the simulation tool is written. It also involved the development and evaluation of each proposed approach by implementing the software code into the simulation code for demonstrating and validating the developed approaches and methods. Due to various resource constraints, it has been simulated by most common and known simulation tool, which is the Network Simulator NS-2 (within the three-year time scale of this research study) for the purpose of evaluation process.

This was followed by step 5 – reflection and feedback, where the problems/limitations and potential refinements for the developed approaches were identified. In the last step, findings were documented and reported. In addition, potential extensions for this study have also been identified for future research and development.

3.2.1 Simulation Environment

The research in this thesis has been simulated by using the Network Simulator NS-2. Kurkowski et al. [88] surveyed the 2000-2005 proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc). They arrived at the result that Network Simulator-2 (NS-2) [89] is the most used simulator in MANET research between all known simulation tools; ("35 of the 80 simulation papers that state the simulator used in the simulation study used NS-2 (43.8%)") as shown in the Figure 3-1.

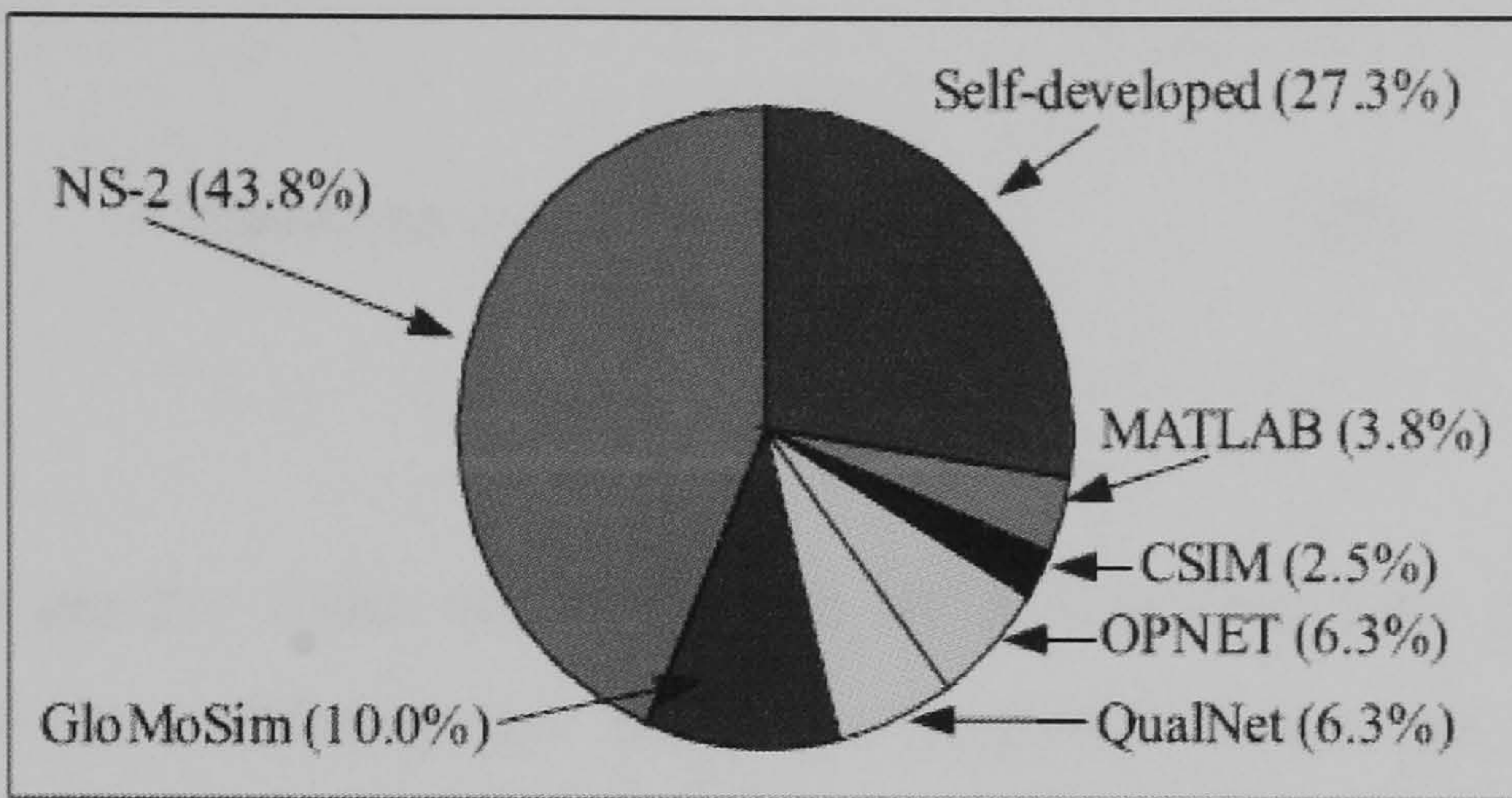


Figure 3-1: Simulator usage from MobiHoc survey [88].

In an attempt to generate results that would be representative of some potential real world scenarios, which the algorithms in this thesis might encounter, simulations ran with parameters values close to the available realistic values. Without lose of generality the protocol evaluations are based on the simulation of 50 wireless nodes for some scenarios, and different number of nodes varies from 10 to 70 for other scenarios. These nodes are forming an ad hoc network, moving about over an area (1000m x1000m) flat space for 500 seconds of simulated time. The square site models situations in which nodes can move freely around each other, and where there is a small amount of path and spatial diversity available for the routing protocol to discover and use. A square space is chosen with size 1000m, which is four times the transmission range in order to get a reasonable number of nodes between the source and destination nodes. This is because a higher number of intermediate nodes results in quicker route breaks. On the other hand, a smaller number of intermediate nodes does not give an indication of the realistic routing protocol. This protocol, in most of the time, needs some intermediate nodes to establish the connection between two communicating node. Another reason for selection the square with length size 1000m is to keep the average number of neighbouring nodes equal or higher than the required number of neighbour in HARP2. HARP2 needs to send the route request packet to one neighbour from each direction zone. The node density equal to 50 / (1000x1000) = 0.00005. The number of neighbour nodes is based on transmission range R and the simulation area:

$$Neighbour\ nodes = \frac{\pi\, x\, R^2}{\frac{w\, x\, h}{n}} \qquad (5)$$

Where w and h are the width and the length of the network area. According to the parameters used for simulating the work, the neighbour nodes are approximately 9 neighbours. The physical radio characteristics of each mobile node's network interface, such as the antenna type, transmit power, and receiver sensitivity, were chosen to approximate the most famous commercially available wireless LAN radio such as Lucent WaveLAN [90] radio. Some famous wireless LAN are presented in table 3-1 [91],

Table 3-1: Wireless LAN Products

Company	Product	Advertised Speed	Advertised Distance
AT&T	WaveLAN	2 Mbps	800 feet
Digital	RoamAbout	2 Mbps	800 feet
NCR	WaveLAN	2 Mbps	800 feet
Solectek	AirLAN	2 Mbps	800 feet

A TCL script file for mobile ad hoc wireless simulations provided with ns-2 distribution has been modified to fit the simulation environment of the project. In this file, it was necessary to define the type for each of the network components that nodes consist of. A mobile node consists of network components like Link Layer (LL), Interface Queue (IfQ), MAC layer, the wireless channel nodes transmit receive signals from, etc. Additionally, in the TCL script file, it is necessary to define other parameters like the type of antenna, the radio-propagation model, the type of ad-hoc routing protocol used by mobile nodes, etc.

The size of trace files generated by running the TCL script file is huge (of the order of tens of MB). These files were analysed to obtain the performance metrics. In order to extract certain lines and discard the rest from the generated trace file for analysis, the AWK utility language was used. AWK is a programming language included with the UNIX operating system that is designed for processing text-based data, either in files or data streams (the name is made from the initials of the three inventors: Aho Weinberger Kernighan). For example, to extract only the information related to only route request packets, it was necessary to write a programming code by using AWK to achieve this task. Writing programming code to do these tasks in languages such as C, C++, or Pascal is time consuming and inconvenient. Such jobs are often easier with AWK. The AWK utility interprets a special-purpose programming language that makes it easy to handle simple data-reformatting jobs, and allows us to extract bits and pieces of data for processing, sort data, and perform simple network communications [92].

3.3 The Key Idea of Heading Direction

This section explores the possibility of using heading information to improve the performance of routing protocols for MANET. As an illustration, this section shows how a route discovery protocol based on mobility information can be improved. Consider two mobile nodes n_1 and n_2 that are within the transmission range R of each other. The (x_{n1}, y_{n1}), v_{n1} and (x_{n2}, y_{n2}), v_{n2} are the coordinates and velocities of n_1 and n_2 respectively. In addition, n_1 and n_2 move in direction θ_{n1} and θ_{n2} from the north respectively (Figure 3-2).

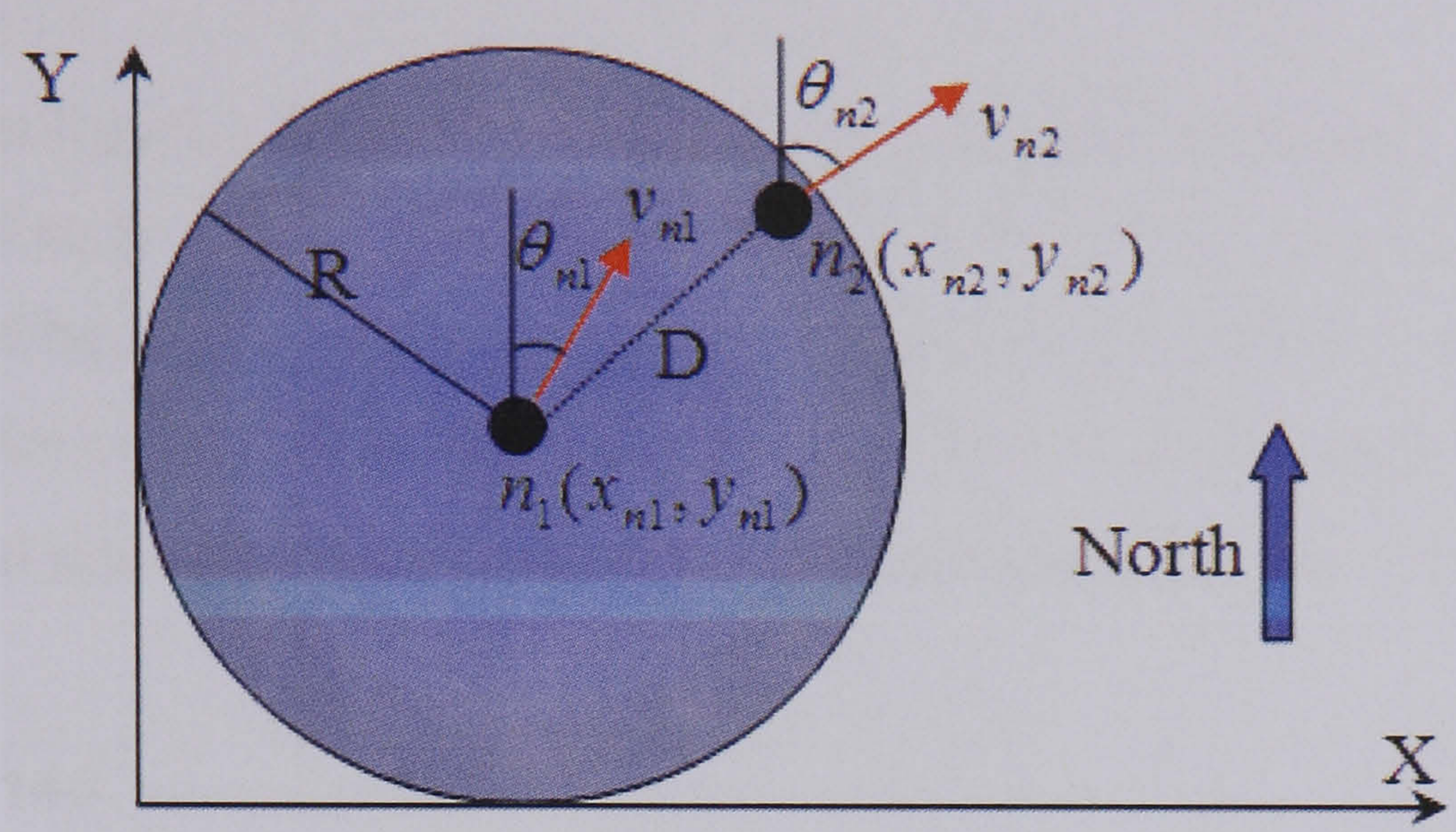


Figure 3-2: Communication Relationship between two nodes in MANET

As can be seen in Figure 3-2, the total time that the two mobile hosts remain connected depends on the difference between θ_{n1} and θ_{n2} as denoted by [8]:

$$T = \frac{-(pl+qd)+\sqrt{(p^2+q^2)R^2-(pd-lq)^2}}{p^2+q^2} \tag{6}$$

where

$$p = v_{n1}\sin\theta_{n1} - v_{n2}\sin\theta_{n2},$$

$$l = x_{n1} - x_{n2},$$

$$q = v_{n1}\cos\theta_{n1} - v_{n2}\cos\theta_{n2},$$

$$d = y_{n1} - y_{n2}.$$

During this time, the distance between the two nodes is changing with time. Note that, θ_{n1} and θ_{n2} are measured with respect to the north, and the link between n_1 and n_2 lasts longer when the two nodes move in similar direction. Figure 3-3 depicts the relation between T and the difference between θ_{n1} and θ_{n2}, with $v_{n1} = v_{n2} = 10$, R = 50, $x_{n1} = y_{n1} = 10$ and $x_{n2} = y_{n2} = 20$

It is clear from Figure 3-3 that the probability of a path break increases as the difference between the direction angles of the end nodes increases. Hence, if the next node in the link is selected based on a similar direction to the upstream node, the link will last longer. If the velocities of both nodes are equal and, $\theta_{n2} - \theta_{n1} = 0$, assuming no other channel conditions will affect the channel link, the time of path breaks increases to infinity.

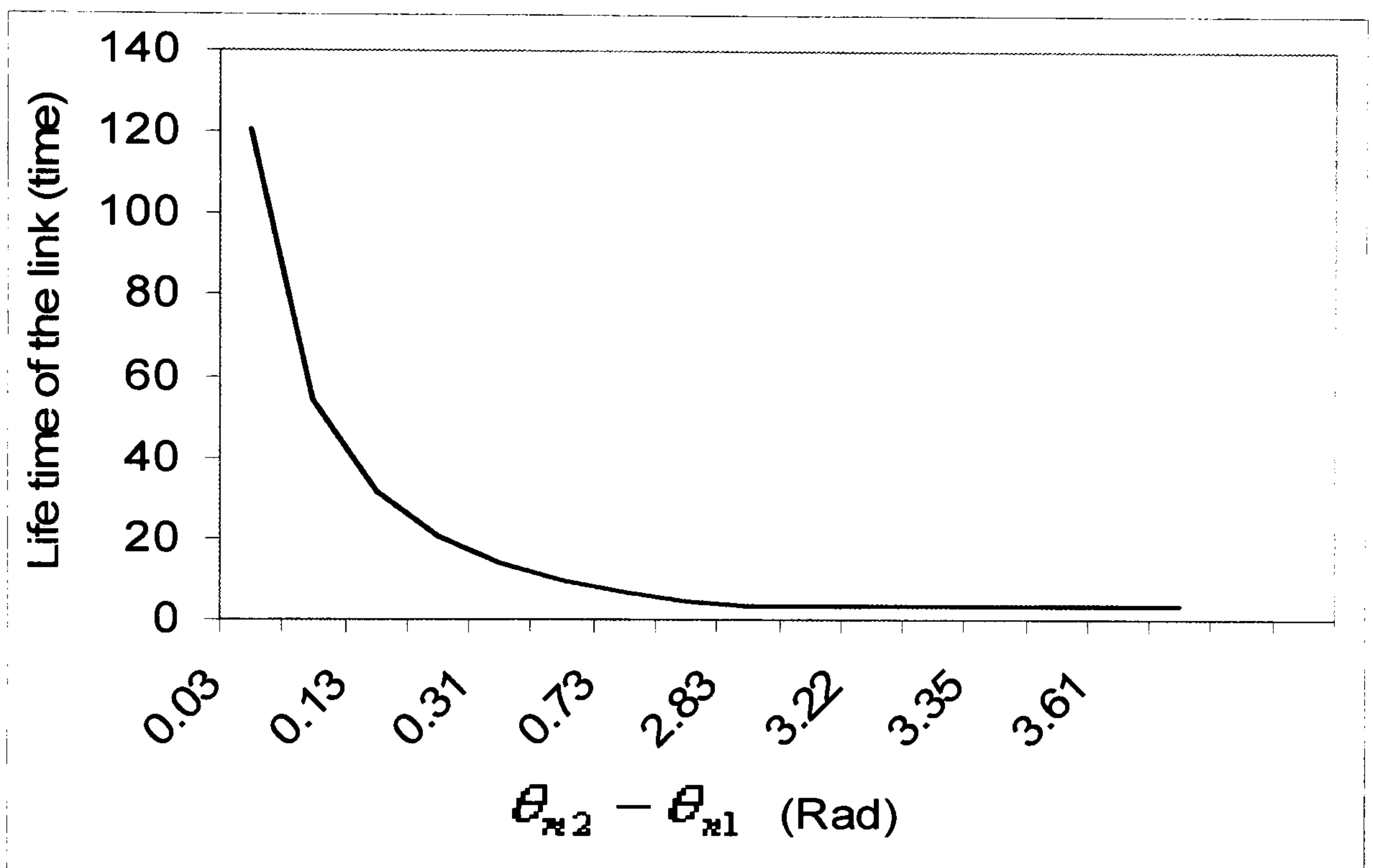


Figure 3-3 The lifetime of the link vs. the difference between the heading angles of end nodes.

In order to apply the idea explained above for selecting the next hop in the route during the route discovery process, extra information is needed. This information source needs to provide the node with the heading direction. This information could be provided by utilising a compass with Magneto Resistive (MR) technology [93]. It delivers the heading direction angle of the mobile device relative to magnetic north. The expected lifetime of a link has been examined by Turgut et al. [71] and Samar et al. [94] where the relation between the lifetime of a link and the difference between the motion angles of two communicating nodes is derived.

Another objective of using the heading direction is that routing protocols that are dependent on external routing information might fail to operate correctly when this information is absent. In addition, routing protocols that rely on geographical information (GPS) [21, 22] may not work properly in every situation. Therefore, an alternative resource of information should be readily available to be used to complete the task of routing.

3.4 The Principle of Heading Direction Mechanism

The core idea of the proposed schemes is termed Heading-direction Angle Routing Protocol (HARP), as it makes use of direction information of nodes in the network. The aim of using the heading direction is to reduce routing overhead and increase the lifetime of links between communicating nodes. It has been assumed that each mobile node in the network knows its heading direction information by using a digital compass with MR technology. Most navigation systems today use some type of compass to determine heading direction. Electronic compasses based on magneto resistive (MR) sensors can electrically determine the change in direction up to 0.1°. They can easily be integrated into systems via a simple communication interface, which makes it ready for use in applications that need such information [93].

The general behaviour of ad hoc networks is to deliver the data packet to the destination through intermediate nodes. Therefore, it is assumed that all hosts wishing to communicate with other hosts in the network are willing to participate fully in the protocols of the network. Each node is willing to receive and forward packets for other nodes in the network. Moreover, each node exchanges its heading direction information with its neighbours in a periodic manner. The information received from another neighbouring node will be stored in the cache memory.

3.4.1 Categorization of nodes

In HARP, each mobile node in the network classifies its neighbouring nodes according to their heading directions into eight different zone-direction groups (z_1, z_2 … z_8). As can be seen in Figure 3-4, each mobile node in the ad hoc network divides the heading directions into different sectors. The heading directions between 0° and 45° are considered as Zone-direction 1 (z_1); the heading directions between 45° and 90° are considered as Zone-direction 2 (z_2), and so on until 360°. For example, consider that a Mobile Node (MN) has a neighbour node moving in a heading direction 30°. The neighbour node is sending its heading direction information to the neighbouring nodes periodically. The MN when it receives the heading direction information from this neighbour will classify this neighbour in zone-direction 1. Theoretically, the neighbouring nodes of a mobile node are categorised within at least one of the eight zone ranges, regardless of their actual relevant positions to the mobile node itself.

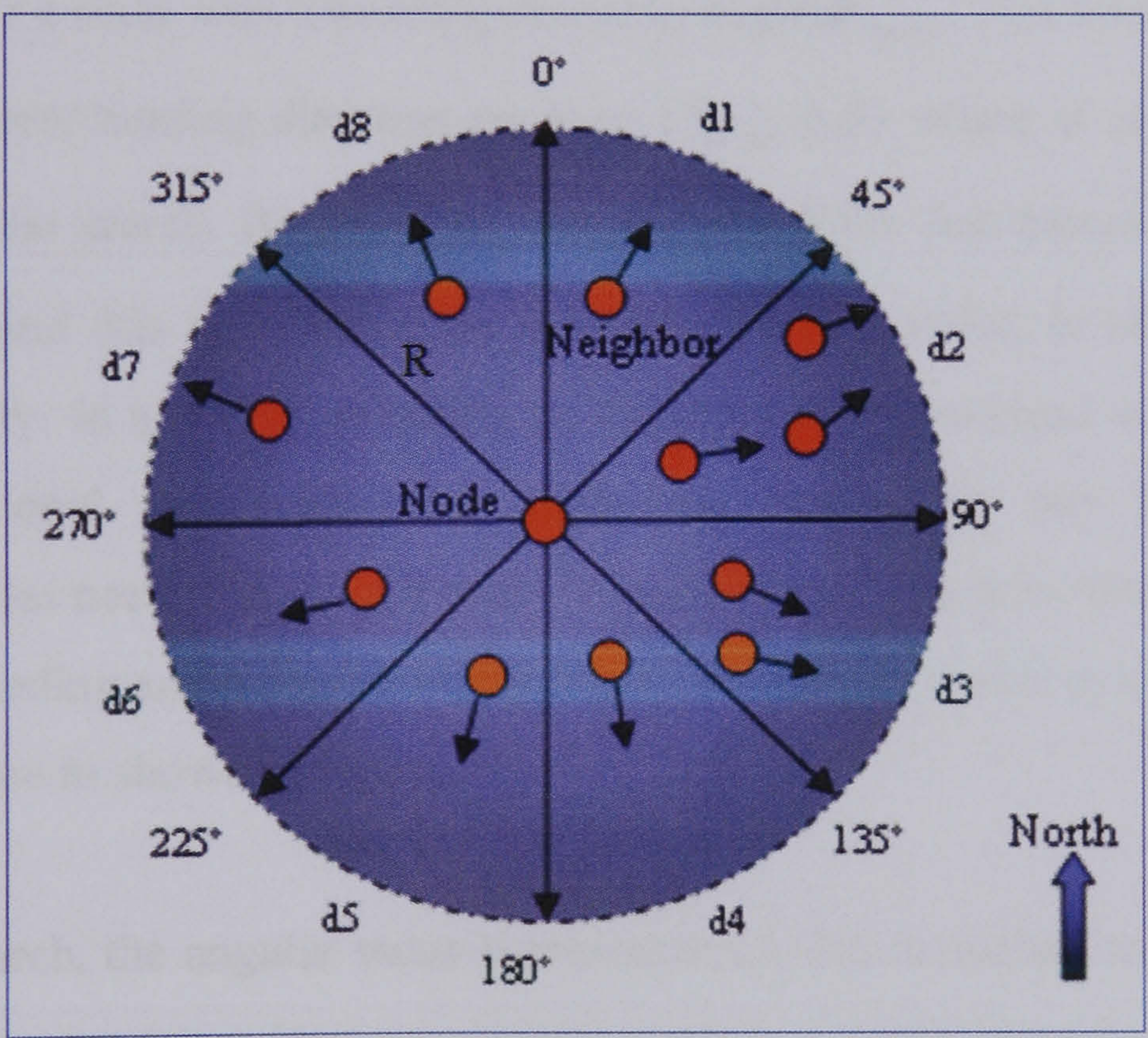


Figure 3-4: The eight basic heading directions ranges and assorting neighbours in these ranges.

3.4.2 Downstream Node Selection

The proposed approaches are based on on-demand routing technique; this means that establishing routes is based on route requests and route replies technique. In other words, when a source node S has data packets to send to a destination D, and in order to find a route to D, the node S will send a RREQ packet. Almost all on-demand routing schemes require that the route request be forwarded toward the destination through intermediate nodes. This means that each node will forward the route request packet to the next downstream node (the next node toward the destination nodes is called downstream node whilst the node from the destination node toward the source node is called the upstream node).

In the proposed approaches, when an intermediate node needs to forward a packet to the downstream node, it selects the downstream node from its neighbouring nodes that are classified according to their heading direction. The selected node has an angular heading direction similar or near to the heading direction angle of the selecting node. For example, consider a node with a heading direction angle, $\theta_{Node\#}$. The selected downstream node has the nearest heading direction angle to $(\theta_{node\#} \pm \delta)$ where δ is an angle around $\theta_{Node\#}$ to expand the search. By doing so, the lifetime of the link between the two nodes will last longer and this is reflected on the routing functionality in that it reduces the effects of mobility. In addition, selecting an appropriate downstream node will result in lower computational overheads and minimised bandwidth use because not all neighbouring nodes need to react to a route request. If the node does not find a neighbour that fulfils the heading angle condition, the search will be expanded by applying the axis-mapping technique as shown in Figure 3-5.

To widen the search, the angular value represented by δ is increased, so a large range of heading directions are taken into consideration when a route request message is being propagated or a route reply message is being sent along already established route.

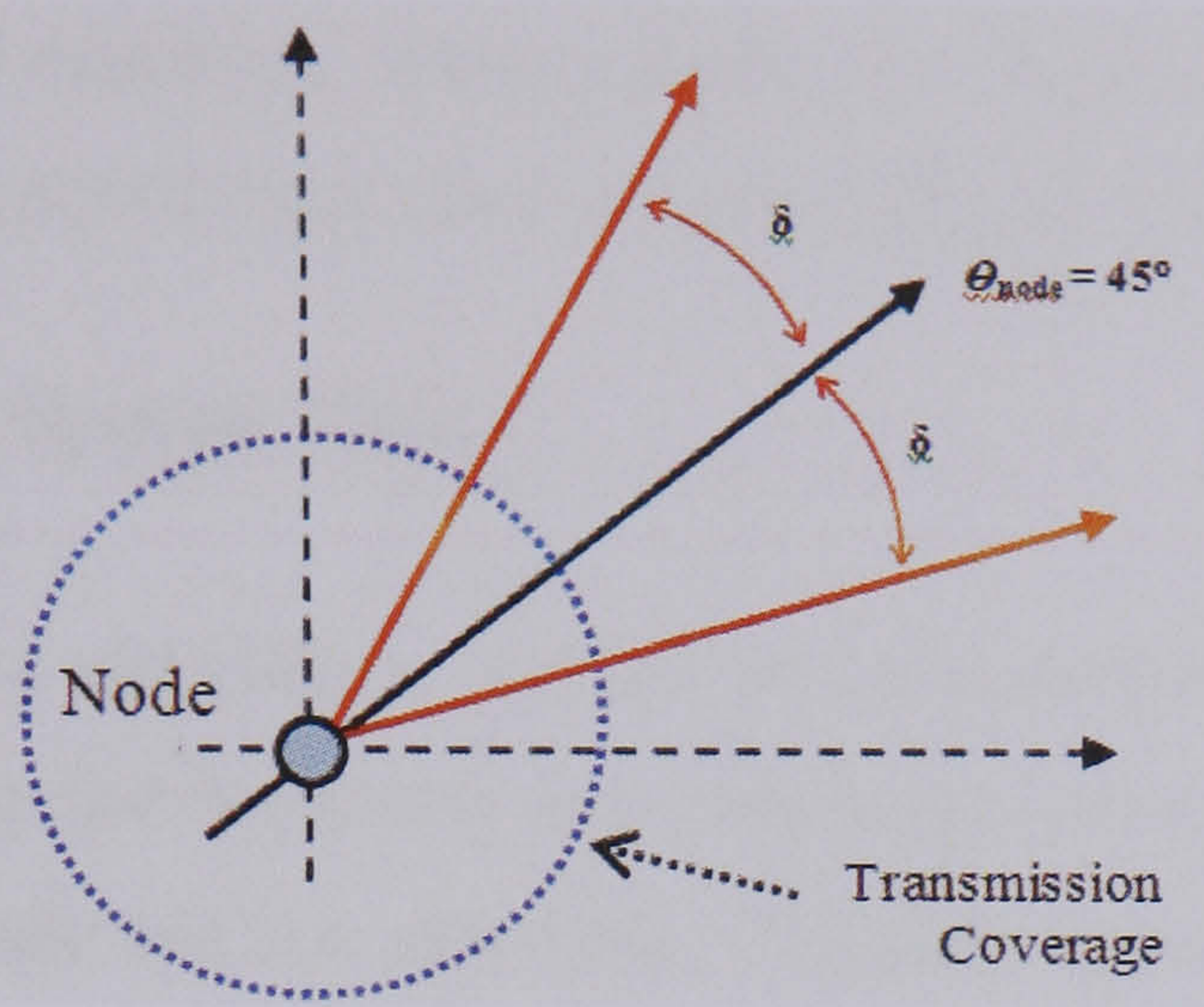


Figure 3-5 Axis mapping technique, δ is added and subtracted along 45°

3.4.3 List of Route Records

The List of Route Records (LRR) consists of a list of records initiated by the source node when establishing the route to the destination node. If the source node has data packets and does not find the destination node in its cache memory (a neighbour table), the source node initiates the LRR list. The source node then adds a record to LRR containing information about itself. Each record of LRR has the following fields:

- A node IP address, which is the IP address of the node that is involved in the route.
- A node-heading angle, which is the heading direction angle of the node itself.
- And a zone-direction number, which is the number of the zone that the heading direction angle of the node is falling in, and has a range value from 1 to 8 (number of zone-direction).

The LRR list is attached in the header of the route request packet and the route request packet is propagated to the proper node(s) depending on the scheme used in routing. During transmitting the route request, each node visited by the route request adds a new record to LRR containing information about the visited node itself.

3.5 Modelling Ad Hoc Network

This section presents the definition of the general system model for the three proposed routing algorithms and describes the network model, mobility model, and traffic model.

In addition, the format of messages, routing tables and the general route establishment mechanism used by the proposed algorithms are also elaborated on.

3.5.1 Definition of the System Model

The three proposed routing algorithms, entitled "the Heading-direction Angles Routing Protocol (HARP)", are intended for use by any mobile devices and have the possibility to work in a peer-to-peer mode (ad hoc network). Complete functions and tasks expected from these protocols have to be achieved via distributed algorithms. These algorithms exploit the mobility of users to offer adaptation to dynamic topology changes and frequent link breaks, low control traffic overhead, elongation of the lifetime of the link, and reduction of the flooding effects. To ensure loop freedom, some other existing routing protocols utilise destination sequence numbers. In addition to the destination sequence numbers, HARP schemes use LRR to add an additional guarantee to ensuring the freedom of the counting-to-infinity problem. Each record in the LRR list contains information about a node involved in the route between the source and the destination node. These algorithms can be adopted by other routing protocols to improve their performance.

3.5.2 Assumptions

Some assumptions have to be made in order to accomplish the tasks of the proposed routing algorithms in this thesis. These assumptions are:

1) Each node is able to get the needed routing information. This information is obtained by direct communication to the resource of information. This resource provides this information whenever it is required. Alternatively, the mobile node is equipped with a device such as a digital compass. This device delivers the heading direction angle of the mobile device hosting it.
2) Each mobile node in the network is willing to exchange the heading direction information with its neighbours in a timely manner. The information received

from a neighbour node will be stored in one of the eight zone-directions in the cache memory regardless of the actual position of that neighbour.

3) The behaviour of ad hoc networks is to transmit data packets through relay nodes between the sender and the receiver. Therefore, it must be assumed that each node in the ad hoc network is willing to forward other nodes' packets beside its own packet.
4) The nodes move in roughly similar speeds such as people on the street.

3.5.3 Models

This section presents three models, the network model, mobility model, and traffic model.

3.5.3.1 Network Model

The multi-hop ad hoc network consists of a set of nodes, *N*. The area of the network, *A* that nodes move in depends on the application and the purpose that the ad hoc network is running. The distribution of nodes in *A* also depends on the scenario that the network is running. The distribution of nodes in the ad hoc network area for some applications can be predetermined such as in classroom, conference, and meeting room, whilst for other applications, the nodes are randomly distributed (such as in search-and-rescue, free user movement). Therefore, the density of nodes in the area (which equals to *(N/A))* varies from application to application and from subsection of *A* to a different subsection of *A*.

Now consider the transmission range of each node is equal to *R*, and every node has an omnidirectional antenna. The transmission/communication between any two nodes n_1 and n_2, (where $n_1, n_2 \in N$) is successful if it satisfies the two conditions:

- If the distance between these two nodes is $d_{n_1n_2}$, the condition $d_{n_1n_2} < R$ should be satisfied;

- If the interference range of the receiving node n_2 is R_{int}, any node ($m \in N$), that is within R_{int} of the receiving node n_2, $d_{mn_2} \leq R_{\text{int}}$ is not transmitting. In general, the transmission range R is the same as the interference range R_{int}.

In the case of IEEE 802.11 MAC protocols [44], the sending node, n_1, is also required to be free of interference as it needs to receive the link layer acknowledgement from the receiving node, n_2. Therefore, in IEEE 802.11MAC protocols, a node m falling in the interference range of the nodes n_1 or n_2, must not be transmitting.

The hidden and exposed terminal problems are generally the concern of the MAC protocols. These problems are not available in wired networks and only occur in wireless networks. The hidden terminal problem occurs due to a simultaneous transmission of those nodes that are hidden from each other or in other words, those nodes are not within the direct transmission range of the sender but are not hidden from the receiver (within the transmission range of the receiver). In this situation, a collision of packets at the receiving node occurs when nodes transmit packets simultaneously without knowing about the transmission of each other. As can be seen in Figure 3-6, both node N_1 and node N_2 try to transmit to node G_1 at the same time. This is because each one of them is not aware about the transmission of other node as both nodes are hidden from each other. This will mean that the both node packets collide at node G_1.

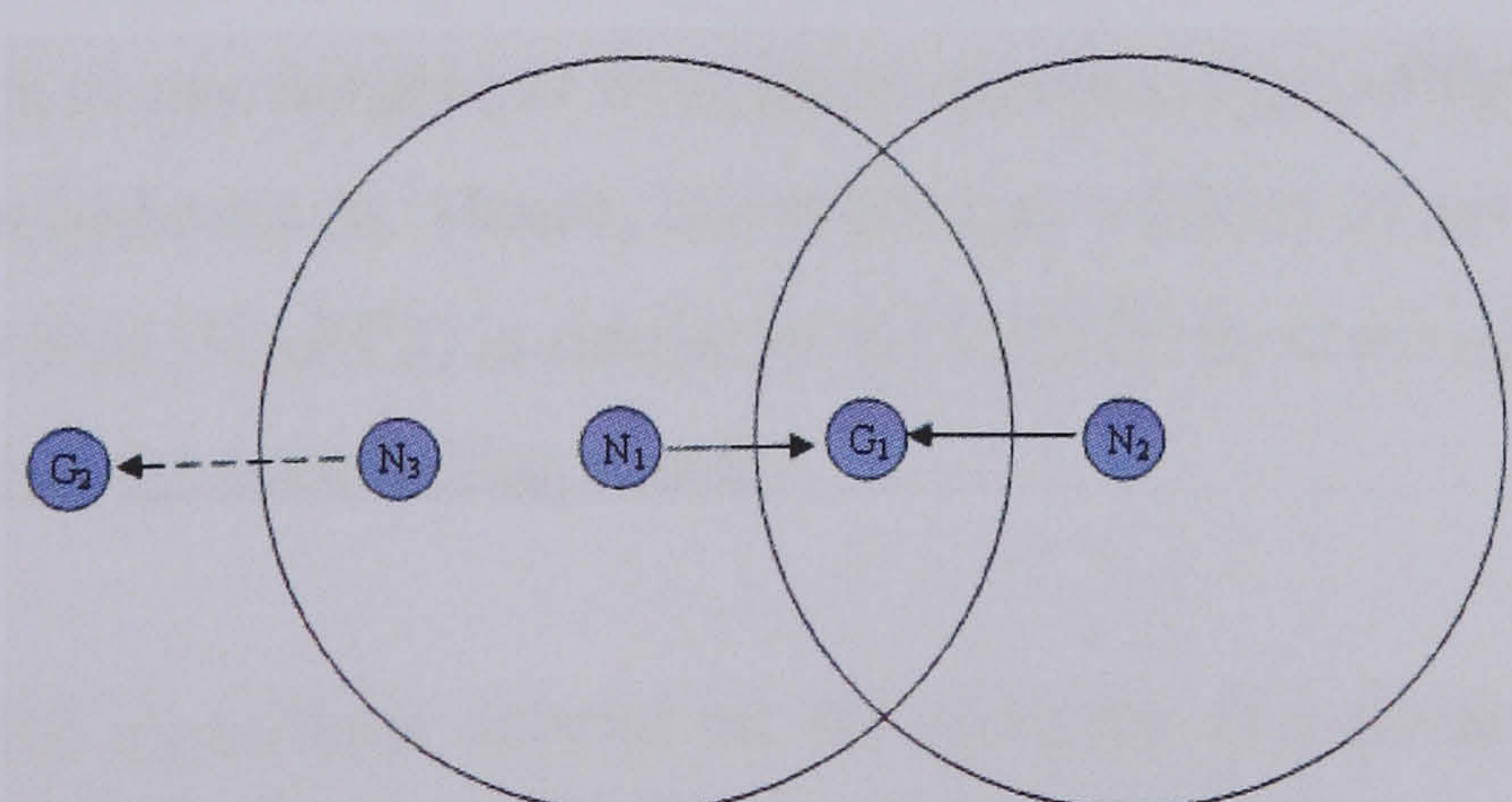


Figure 3-6 the hidden and exposed problems in ad hoc network.

The exposed terminal problem is the phenomenon of blocking one node from transmitting by another node due to a nearby transmitting node. In Figure 3-6, the node N_3 cannot transmit to node G_2 because the transmission from node N_1 to another node G_1 is already in progress and the transmission of N_3 would interfere with the on-going transmission of node N_1.

The performance of ad hoc networks is reduced by the occurrence of the hidden and exposed terminal problems, especially when the traffic load is high. Therefore, when designing and developing a MAC protocol, it should take into account the potential hidden and exposed terminal problems and take appropriate measures.

3.5.3.2 Mobility Model

The HARP algorithms are proposed for mobile ad hoc networks with a minimum number of mobile nodes, which varies with the scheme used in routing. Each of the three proposed algorithms requires a different minimum number of nodes in the network to guarantee establishment of the route from the source node to the destination node. The first algorithm is termed HARP1. In HARP1, each node sends a Route Request packet (RREQ) to only one neighbour. Hence, a low density of nodes is acceptable but, of course, the higher the number of available neighbours to select from, the more appropriate the selected neighbour will be, which increases the performance of HARP1. In second algorithm, termed HARP2, the source node needs to forward a RREQ message to one neighbour from each direction zone of the zones that the source classifies its neighbours in. Hence, the minimum number of nodes is eight. The third proposed algorithm (HARP3) is similar to the HARP1 in terms of the minimum number of nodes required for establishing routes.

Since the HARP algorithms depend on the direction movement of mobile nodes and they are on-demand algorithms, they can handle low, moderate mobility rates. Clearly, in ad hoc networks, mobility models are application dependent. Moreover, the various mobility patterns affect the performance of different network protocols in different ways. For example, the performance of the routing protocol under the scenario of the group mobility model (such as in a highway and military group) varies in performance if it runs under random mobility model or random walk mobility model.

The random mobility model is the most common model used by researchers. In the Random Waypoint mobility model [74], nodes are randomly placed within the simulation field at starting time. Each node selects a destination randomly and independently from other nodes, to which it moves with a constant speed. When a node reaches the destination, it stays there for a given pause time before it starts to move to another random destination. In the HARP algorithms, selecting the appropriate next node during establishing the route depends on the heading direction information. Hence, the mobility model is not strongly affected by the performance of these algorithms because the adaptiveness with the direction of movement where the node selects the next node that is moving in similar direction to the current node. For example, in group mobility scenario, all nodes move in a determined direction so the next node is selected from this group easily and there are more choices in selecting the next node, since all nodes move in similar direction. Using the random scenario, there are still neighbour nodes to select from, with near similar direction to the current node.

3.5.3.3 Traffic Model

The physical model is directly related to the physical layer characteristics. The transmission from node n_1 to n_2 is successful if the Signal-to-Noise Ratio (SNR) at node n_2, SNR_{n1n2}, is not less than a minimum threshold: $SNR_{n1n2} \geq SNR_{thresh}$. Since the work in this thesis is related to the network layer, the physical model is beyond the scope of this discussion, and left as a future research direction. As it is assumed that each mobile node has an omnidirectional antenna model, the propagation model combines both a free space propagation model and a two-ray ground reflection multipath model. In the free space, the power of a signal attenuates as $1/d^2$ where d is the distance between the transmitter and the receiver. For this work, it is assumed that the propagation range of mobile nodes is equal.

3.5.4 General System Model

This section describes the messages used by the HARP algorithms, routing tables used to maintain the routing information, and the general route establishment mechanism.

3.5.4.1 Message Formats

In the proposed algorithms, as in other routing algorithms of mobile ad hoc networks, a number of messages are used to perform the task of running the algorithm. These messages are used to establish routes and for sending data packets from a source node to a destination node. The required format for each message, the fields that each message consists of, and the contribution of each message in the achievement of routing in mobile ad hoc networks is described.

3.5.4.1.1 List of Route Records Format

In the List of Route Records (LRR), each record contains the node IP address, the node heading direction angle, and the node zone-direction number. Each node in the network contributed in setting up the route and those involved in forwarding the data packet to the destination has a record in the list. This list is constructed during the stage of finding the path to the destination. An additional task of this list is to share with the destination the sequence numbers preventing the counting-to-infinity problem. Other details about LRR are explained in subsection 3.4.3. The fields' names of LRR list used in the proposed approaches are shown in Table 3-2.

Table 3-2: List of Route Records Format

Field Name	**Description**
rl_nodeIP	A node IP address
rl_nodedir	A node heading angle
rl_zonerange	A zone-direction number (1-8)

3.5.4.1.2 Route Request Message Format

If the destination node is not a neighbour to the source node, the route request message is initiated and prepared by the source node with the necessary information before transmitted onto the network. In general, the common main necessary fields required in the RREQ message are the source and destination IP addresses, the LRR list, and the packet type to differentiate between the packet types (Route Request, Route Reply, Route Error, and Hello Message). The HARP3 scheme in this thesis utilises the geographical location of the destination; hence the destination location is included in the RREQ message. The general fields' names used in the RREQ message are shown in table 3-3:

Table 3-3: Route Request Message Format

Field Name	**Description**
rq_type	Packet Type
rq_bcast_id	Broadcast ID
rq_dst	Destination IP Address
rq_dst_seqno	Destination Sequence Number
rq_dst_X	Destination X Coordination (for HARP3)
rq_dst_Y	Destination Y Coordination (for HARP3)
rq_src	Source IP Address
rq_src_seqno	Source Sequence Number
rq_timestamp	when RREQ sent; used to compute route discovery latency
rq_rt_list	List of route record

3.5.4.1.3 Route Reply Message Format

The Route Reply message is initiated and prepared with necessary information by the destination node or by an intermediate node, which has a fresh enough route to the destination node. The RREP is then unicasted back to the source node that generated the RREQ. In all proposed schemes in this thesis, the RREP message consists of identical fields. In general, the main fields required in the RREP message are the source and destination IP addresses, the LRR list, the packet type to differentiate between the packet types. Here, it is important to notice that the field Destination IP Address is the node that generates the RREQ message, and the field Source IP Address is the node that generates the RREP message. The general fields' names used in the RREP message are shown in Table 3-4.

Table 3-4 Route Reply Message Format

Field Name	**Description**
rp_type	Packet Type
rp_dst	Destination IP Address
rp_dst_seqno	Destination Sequence Number
rp_src	Source IP Address
rp_lifetime	Lifetime
rp_timestamp	When corresponding REQ sent; used to compute route discovery latency
rp_rt_list	List of route record

3.5.4.1.4 Route Error Message Format

The route error message is initiated and prepared by an intermediate node when a broken link to the next node is discovered. In addition, RERR is initiated at the expiration of the time required to find the destination without reaching to the destination yet (a further explanation is in the next sections). The route error message is filled with necessary information before it is unicast to the network toward the source node that generated the RREQ. In all proposed schemes in this thesis, RERR message consists of the same fields. The RERR message should contain all the IP addresses of the nodes that are not reached anymore due to the occurred error. Those unreachable nodes should be accompanied with their sequence numbers. The general fields used in the RERR message are shown in Table 3-5.

Table 3-5 Route Error Message Format

Field Name	**Description**
re_type	Packet Type
re_DestCount	Destination Count
re_unreachable_dst[]	List of Unreachable destination IP addresses
re_unreachable_dst_seqno[]	Unreachable destination sequence numbers

3.5.4.1.5 Hello Message Format

Selecting the next hop according to the heading direction of the next node requires that the node should be aware of the heading directions of its neighbour nodes. Each node in the network is required to broadcast local hello messages with one hop distance every Hello interval time. The determined value of the interval time should be a compromise between the local control overhead and the information update frequency. Before determining that the neighbour does not exist as a neighbour anymore because there are no more hello messages being received from it, it should be allowed a number of lost messages.

In general, the main fields required in the RREP message are the node IP address accompanied with its sequence number, and the node heading direction angle. The HARP3 scheme in this thesis utilises the geographical location information; hence, the node location is included in the HELLO message. The general fields used in the HELLO message are shown in Table 3-6.

Table 3-6 Hello Message Format

Field Name	**Description**
hl_type	Packet Type
hl_IP_Node	Node IP Address
hl_Node_seqno	Node Sequence Number
hl_hop_count	Hop Count
hl_nodedir	Node direction
hl_nodeX	Node X Coordination (for HARP3)
hl_nodeY	Node Y Coordination (for HARP3)

3.5.4.2 Tables Formats

This section describes the format of the routing table used by the proposed algorithms. These tables maintain the routing information used for establishing routes between nodes and for keeping information about neighbours.

3.5.4.2.1 Routing Table Format

Since the HARP algorithms are on-demand routing protocols, it should be noted that each algorithm needs a routing table to keep information about all known routes. The routing table also needs special algorithm management such as adding new route, deleting expired or broken routes, and searching in the table for a route to known destination.

The routing table is a collection of records where each record contains the following main fields: the destination IP address that represents the destination node reachable by this node itself, the sequence number correspondent to the destination, the number of hops that forms the route to that destination, the IP address of the next hop in the route to that destination, and the time of expiration the route to that destination(the time when the information stored in this record become stale information). The general fields' names of routing table at each node are shown in Table 3-7.

Table 3-7 Routing Table Format

Field Name	**Description**
rt_dst	Destination IP Address
rt_seqno	Destination Sequence Number
rt_hops	Hop count
rt_nexthop	Next hop IP address
rt_expire	Expiration of the route

3.5.4.2.2 Neighbours Table Format

The information about the neighbouring nodes extracted from received messages is stored in the neighbours table. The Hello message sent by a node to its entire neighbours (one hop away) contains the node IP address, the heading direction of the node and the calculated zone number that the node fall into. This information received by a neighbour will be stored in the neighbours table as a new record if the neighbour is not previously stored or will be modified if the neighbour is already available in the table. The RREQ and RREP messages received from the neighbour node will also cause the information of that neighbour in the neighbours table to be added as new record if the neighbour is not previously stored. Alternatively, the information is modified if the neighbour is already available in the neighbours table.

The neighbours table is a list of records, where each record contains the main fields: the neighbour IP address; the heading direction angle of the neighbour; the number of zone-direction that the neighbour falls into; and finally the time that this information is expired and became obsolete. The number of zone-direction ranges from 1 to 8. The neighbours table also needs special algorithm management such as adding new neighbour, deleting expired neighbour, and searching in the table for a neighbour by its IP address or by the heading direction angle, or by the zone number. The general fields' names of neighbours table used in our approaches are shown in Table 3-8.

Table 3-8 Neighbours Table Format

Field Name	Description
nb_addr	Neighbour IP Address
nb_dir	Neighbour Heading Direction
nb_zonerange	Neighbour Zone Number (1-8) that neighbour belong to
nb_expire	Expiration of the Neighbour

3.5.5 Route Establishment

The HARP algorithms are classified under the on-demand/reactive routing protocols class. This means that the source node discovers the route only when it is needed. On-demand routing protocols are different from other classes that each node in the network is aware about the whole network information and changes. On-demand protocols maintain only the already discovered routes and use them if they are not expired. The source node will directly send the data packets addressed to the destination without establishing a path to that destination in the following cases:

- The destination is a neighbour to the source node.
- There is a readily valid route to the destination in the routing table that is not expired at the time of sending the data packets.

In all other cases, the operations of establishing a route to the intended destination are triggered. In addition, as an improvement to the proposed algorithms performance, the Local Broken Route Repair (LBRR) algorithm is implemented in the three proposed algorithms. Data packets intended to reach a destination node should be buffered in the node until an active path to the destination is available. Otherwise after a predetermined waiting time for finding a path is passed, the data packets should be dropped and a notification message should be sent to the application from which the packets are generated. The general common route establishment in the three proposed algorithm are mentioned in the following subsections as part of the model explained in this chapter.

Specific Details and some changes about route establishment for each proposed scheme are discussed in the coming chapters related to each scheme.

3.5.5.1 Route Requests

When the source node *S* has data packets to send to a destination node *D*, it first looks into its cache whether the destination could be reached either as a neighbour to *S*, or by valid route to *D*. Otherwise, *S* needs to setup a path to *D*. Preparing and broadcasting the RREQ packet for finding the path to *D* could be divided into two parts:

1) General information that every RREQ packet should contains, and this information could be classified as two types:
   a) Route information that is contained in the packet during its life and trip in the network such as:
      - The destination Sequence Number: the last known destination sequence number for *D*
      - RREQ ID: increment by one from the last RREQ ID used by the current node. This ID together with the originator IP address prevents the node from receiving and reprocessing the same packet more than once.
      - The hop count. To count the number of visited nodes starting from the sender.
      - Time to live value.
      - The originator IP address
      - The destination IP address
      - The destination coordination, X, Y, and Z (for one of the proposed schemes)
      - List of Route Record (LRR). Explained earlier

   b) RREQ information that is kept at the source node itself to control the generation and propagation of RREQ packet such as:
      - RREQ ID

- Maximum of RREQ tries: the maximum number of broadcasting the RREQ in order to find the required route. Every time the RREQ broadcasted, the RREQ ID is incremented.
- RREP waiting time: a waiting time for a RREP for the destination that the RREQ was sent to. If no RREP is received within the waiting time the node may again try to broadcast another RREQ if the numbers of tries dose not exceed the maximum number of RREQ tries.
- The heading direction angle of the node itself.
- The zone number of heading direction that the node fall into after finding the zone number by knowing the heading direction angle.

2) RREQ broadcasting technique: it is determined by the protocol itself such as blind flooding, partially flooding, and controlled flooding. In the AODV protocol, RREQ messages are flooded to all neighbouring nodes and those, in their turn, flood the received RREQ again to their neighbour nodes. In the work in this thesis, the selective and controlled flooding technique is used. Each HARP algorithm has a different technique of broadcasting the RREQ packet to other nodes in the network. These techniques are elaborated on later in next coming chapters.

3.5.5.2 Route Replies

After receiving the RREQ by a node, the route reply packet will be generated in two cases:

- The node is the intended destination
- The node has a valid route to the destination in the routing table and the route is not expired

Before unicasting the RREP back to the source node that generated the RREQ, the node should prepare the RREP packet with the necessary information. This information is extracted from the received RREQ and are:

- The originator IP address

- The originator Sequence Number
- The destination IP address
- The LRR list

After that, the node increments its own sequence number to be greater than the one in RREQ. Moreover, enter the value zero into the Hop Count of RREP. The RREP is propagated unicastly to the next hop indicated by the last record in LRR toward the originator of RREQ.

When receiving a RREP packet, the node first checks whether the RREP is addressed to this node. If not, it discards the RREP, otherwise, the node resets the "soft state" maintained for route in the routing table. The node checks if it has a route to the destination. If not, the route is added. Otherwise, the existing route is updated by updating the destination sequence number and the hop count to that destination. If the node has data packets to this destination, it starts forwarding them to the destination. Finally, the RREP is sent to the next hop IP address available in LRR.

3.5.5.3 Route Errors

In general, invalid route to destination could occur in two cases:

1) The received data packet contains an unknown destination
2) The route is not previously established, or is already established but expired, or a link between the node and next node in the route is broken due to some reasons. These reasons could be node mobility, fading environment, signal interference, high error rate, and packet collisions. A node detects a link break when it receives a link layer feedback signal from the MAC protocol, or it does not receive passive acknowledgments.

A route error message is raised in the following cases:

- The period T_d (the time required to find the destination by RREQ) is expired at intermediate node during route request.

- The period T_n (T_n is the time required by a node to find its neighbours) is expired and the intermediate node did not hear or finds any neighbour.
- At a broken route, if a downstream node cannot find the upstream neighbour that has a record in the list of route records. This error is triggered after the fail of Local Broken Route Repair algorithm to solve the problem caused the error.

Preparing a RERR packet before sending requires the filling the following information into the RERR:

- The all IP addresses of unreachable destinations that are reached by the broken route or invalid next hop.
- If the broken route is already in the routing table, its Destination Sequence Numbers should join the IP addresses filled in the previous step by filling the field "Unreachable destination sequence numbers" in the RERR packet. This field has a zero as initial value.

When a node receives a RERR packet, it searches for a route to the unreachable destination in its routing table. If a route exists and the next hop listed in the routing table entry is the node that sent this RERR then the route is invalidated.

3.6 Summary

In this chapter, the general system model for the three proposed routing algorithms has been presented. Conditions that have to be fulfilled in order to accomplish the tasks of the proposed routing algorithms are also listed. The environment that the proposed algorithms are designed to work into is described by the network model, the mobility model, and the traffic model descriptions. The format of control messages used in these algorithms to perform the task of establishing routes and controlling data packets transmission between mobile nodes are discussed with details. In addition, the routing tables used by nodes to maintain the received information about the known routes and the neighbouring nodes are presented showing the general information contained in these tables. Moreover, this chapter describes the general method shared between the HARP algorithms for establishing routes. The general system model discussed in this chapter will be elaborated on in coming chapters, in which the HARP algorithms are described in detail. In the next chapters, when presenting the new algorithms, the differences between the general model described in this chapter and the specific model that is applied to the algorithm will be highlighted. Hence, the model given in this chapter is considered as the reference model for the coming three chapters.

Chapter 4
HARP1 (Heading-Direction-Based Routing Protocol)

4.1 Background and Motivation

In this chapter, a novel routing approach for multiple-hop mobile ad hoc networks is presented. Research into ad hoc networks has yielded considerable advances over the past few years, particularly in the areas of developing and designing new routing techniques [3]. Nevertheless, significant deficiencies of ad hoc networks remain, especially when compared with infrastructure networks. In mobile ad hoc networks, the only possible direct communication is between neighbouring nodes due to the limited transmission power of the devices; therefore communication between remote nodes is based on multiple-hop. These nodes are mobile, so the interconnections between nodes are capable of changing on a continual basis. Due to mobility, the most important role in routing protocols in mobile ad hoc networks is finding and maintaining robust and long-lived routes between sources and destinations. When designing a routing algorithm, the essential requirements that the routing algorithm has to meet are keeping the routing table reasonably small, choosing long-lived route for given destination and requiring small amount of control messages to converge.

As mentioned in the previous chapter, serious impediments of mobility in MANET are the increasing rate of link failure with increasing mobility of nodes, and activation of links. This increases both the congestion due to traffic backlogs and the volume of control traffic required to maintain routes. Thus in order to achieve adaptive routing responsiveness and efficiency, the main goal of designing HARP1 protocol is to reduce the reaction to mobility.

The approach proposed in this chapter takes advantage of mobility of mobile nodes to establish a robust and long-lived route between sources and destinations. This is in addition to reducing the flooding and overhead effects and minimizing the rate of links breakage in the established paths. In the proposed approach, selecting nodes to forward packets between the source and the destination nodes is based on the HDA of these nodes. Several routing approaches have already been proposed with the aim of avoiding or reducing problems posed by mobility of nodes in mobile ad hoc networks, such as frequent unpredictable topology changes [6-8].

It has to be borne in mind that the proposed approach could be used as a stand-alone routing protocol under the limits and environment discussed in the Modelling ad hoc network chapter (chapter 3) and in this chapter. It could also be adopted by other existing routing protocols in order to obtain long-lived routes and enhancing the performance of these protocols.

4.2 HARP1 Routing Protocol

This chapter presents the operation of the first proposed Heading-direction Angle Routing Protocol (HARP1) that I have conducted through my research [95]. HARP1 is an on-demand routing protocol, which can be considered as two parts: the first part is the mobility and nodes classification, whilst the second part is the route discovery and maintenance.

4.2.1 Mobility and Nodes Classification

As mentioned previously in chapter 3, in HARP1 each mobile node sends its mobility information to its neighbouring nodes in a periodic manner. Therefore each mobile node in the network will be able to classify its neighbouring nodes according to their heading directions into eight different zone-direction groups (z_1, z_2 ... z_8) as each mobile node divides the heading directions into different sectors. The neighbouring nodes of a mobile node are categorised within at least one of the eight zone ranges, regardless of their actual relevant positions to the mobile node itself.

4.2.2 Route Discovery

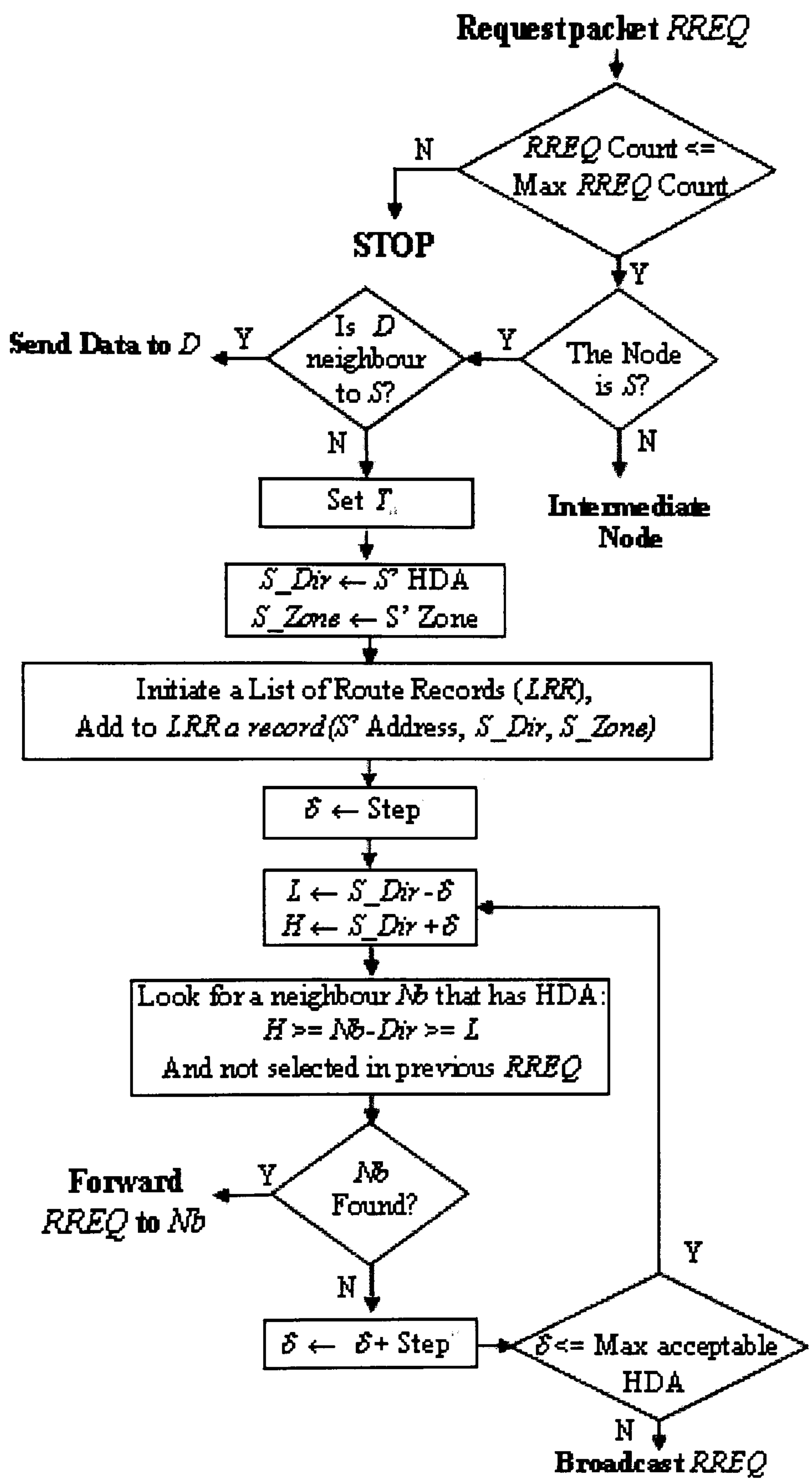
This section includes description of the route discovery initiated at the source node and the intermediate nodes (the intermediate nodes are all nodes except the source and destination nodes). It also includes the route maintenance and local repair mechanisms that are executed when a link is broken.

4.2.2.1 Route Discovery at the Source Node

HARP1 considers that the source, *S*, does not know the geographical information of the destination, *D*, and all mobile nodes in the networks do not have location information about each other. At the source node, when a source *S* requests route to a destination *D*, it will look in its cache for the destination node, and if the destination node is found as a neighbour in its cache, *S* will start forwarding the data packets to *D*. If *D* is not found in the source cache, a time T_d will be set up by the source *S*, where T_d is the determined time required to find the destination. *S* then starts looking into its cache for a neighbour that has a reference or near reference angle, matching with or close to the heading direction angle of *S*, (in order to elongate the life time of the route).
Therefore, for best matching and finding a neighbour with nearly similar heading direction to the node itself, it could be seen in Figure 3-3 that this protocol performs well in a network where nodes form groups, where each group moves together in one direction such as in military, vehicles on highway, and so on.

This protocol enhances other existing routing protocols that use flooding the route request across the network to reach to the destination target by controlling the flooding by the nodes that let the link last longer.
Here, after searching for a neighbour in the cache memory of *S*, there are two possibilities:

1) If *S* did not find a neighbour in its cache; axis mapping [96] will be applied with increment an angle value $\pm\delta$ around the heading angle of *S*, to widen the search for another neighbour in a new direction. If no neighbour is found in the time T_d, a route request (RREQ) will be triggered again (*S* will repeat the route request for a limited number of times, to avoid the search-to-infinity, while excluding neighbours that have been selected in previous tries of finding *D*.



Flowchart 4-1 Route discovery at a Source node S

2) If S finds a neighbour in its cache (in case more than one neighbour is found, the nearest to S direction will be selected); a *LRR* is initiated by S and adds its information record to that list. Then the route request message will be propagated

along the chosen heading direction angle of a neighbour node to that neighbour. Flowchart 4-1 presents the steps followed at the source *S* that has data packets to send to node *D*. in Flowchart 4-1, the *Max RREQ Count* is the maximum number of RREQ allowed to be sent for searching for a particular destination *D*. *S_Dir* is the heading direction angle of the source *S*, and *S_Zone* is the zone of *S* (Zone1 between 0^o and 45^o, Zone2 between 45^o and 90^o, and so on). *Nb_Dir* is the heading direction angle of the neighbour *Nb*, and *Max acceptable HDA* is the maximum accepted angle around the HDA axis of node that the node uses to search for a neighbour.

In this work, the directions have been divided into eight zones, but could be divided to different number of zones if necessary. For example, in a high-density network, the possibility of finding a neighbour in a small direction zone is high, hence grouping the nodes in a greater number of zones allows for greater efficiency in finding the optimum neighbour.

4.2.2.2 Route Discovery at the Intermediate/Relay Node

At intermediate nodes, all the nodes that receive the route request message update their route cache entries by updating the information of the neighbouring node which the message was received from, and only the intermediate node that the message is addressed to, will accept the received route request message. Other nodes will silently drop it. The intermediate node that the message is addressed to, will search in its cache of neighbours for the destination *D*, and:

1) If *D* is found in the cache memory, the intermediate node will update the *LRR* list by adding a record at the end of the list containing information about the intermediate node itself, then it propagates a reply message along the nodes that have records in *LRR* backtracked to the initiating source *S*.

2) If *D* is not found in the cache memory, axis mapping will be applied with an increment an angle value $\pm\delta$ around the heading angle of *S*, to widen the search for another neighbour in a new direction. Before forwarding the route request

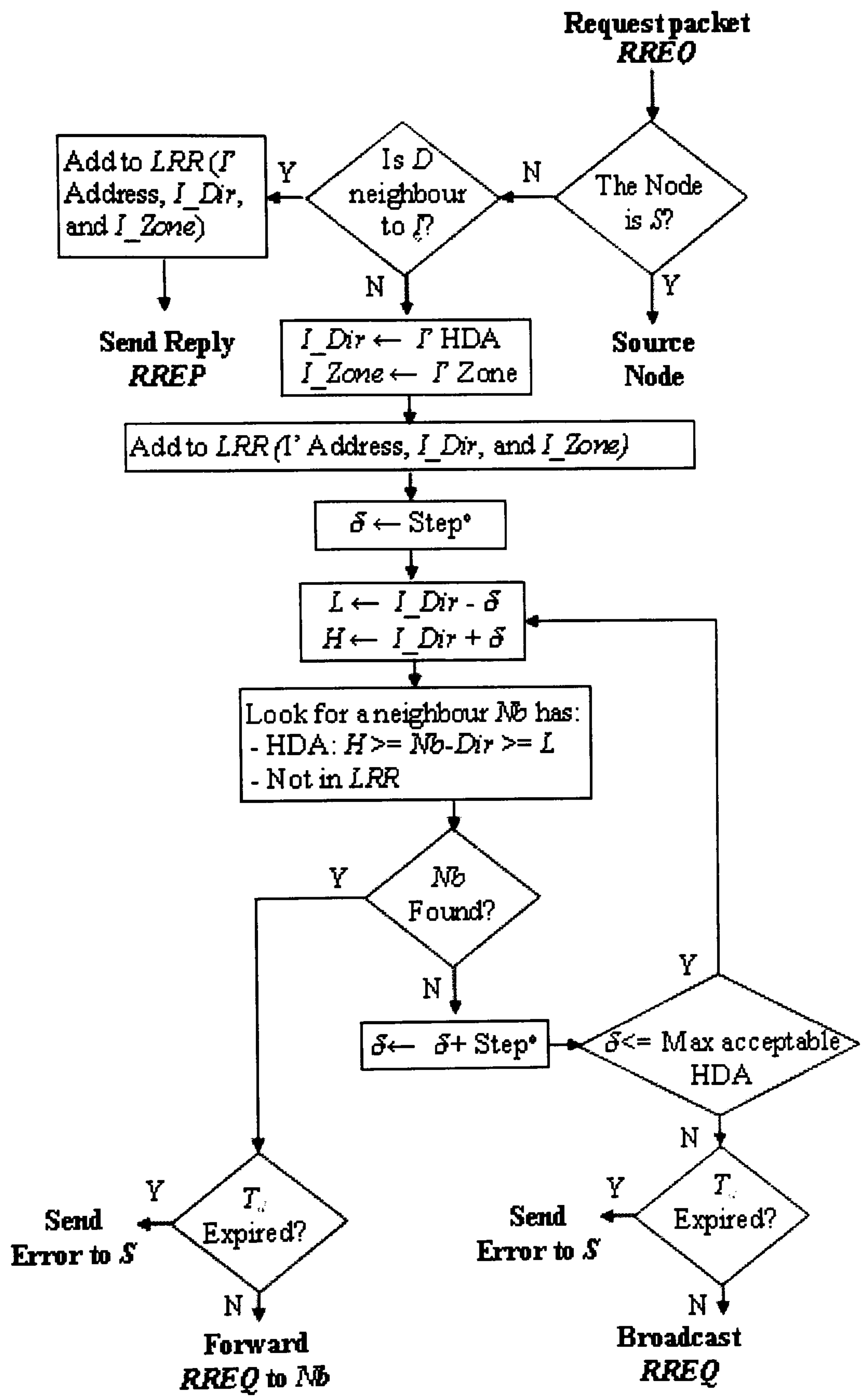
message, the intermediate node will add a record to *LRR* containing information about the node itself. Flowchart 4-2 presents the process actions at the intermediate node.

4.2.2.3 Route Reply

Route reply message would be triggered in two cases:

1) By the destination itself, when the destination *D* receives the route request packet, *D* will piggyback the *LRR* that is included in the route request, in the replied message and send the message along the reversed path determined by the nodes recorded in *LRR*.
2) By an intermediate node, which has received the route request message and has information about the destination stored in its cache (a valid path to the destination). In this case, the intermediate node will update *LRR* by adding its information and piggyback the LRR in the replied message, and then send the message along the reversed path determined by the nodes recorded in the list *LRR*.

An example of propagating a route request from the source *S* to the destination *D* in HARP1 is shown in Figure 4-1.



Flowchart 4-2 Route discovery at an Intermediate node *I*

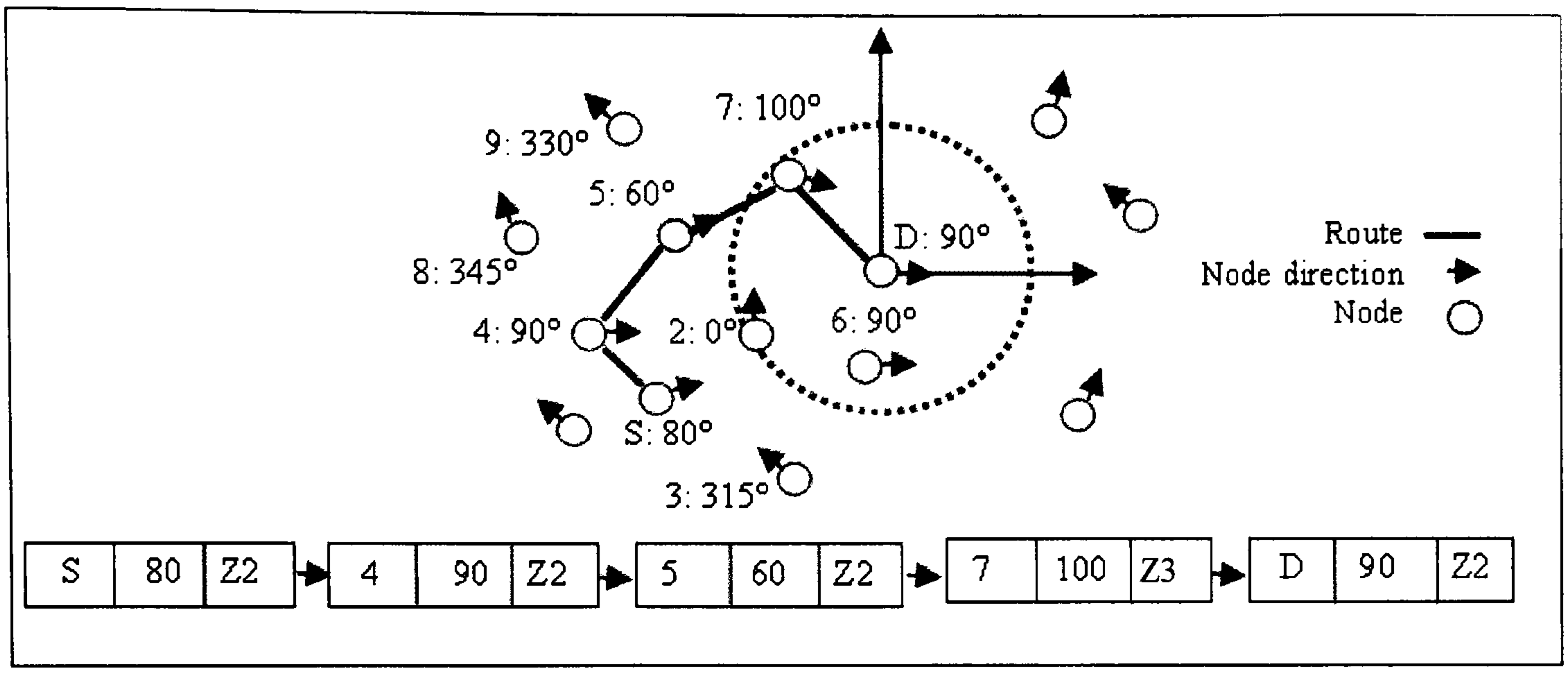


Figure 4-1 propagating a route request from the source *S* to the destination *D*

As can be seen in this figure, the source *S* moves in heading direction 80°. Therefore, according to the rule of selection the next hop to forward the route request packet to, *S* selects node 4. Node 4 then follows the same rule of selecting the next downstream node, which is node 5, and so on. The LRR shown down the bottom of this figure is the information of nodes that the path is consist of. The first record represents the source node *S*. The first filed is the node identity, the second field is the heading direction, and the third is the zone direction that the source fall into.

4.2.3 Route Maintenance and Local Repair

Route Maintenance is a mechanism used to detect the change in ad hoc network topology that leads to the broken route used by the packets using that route for sending or forwarding a packet to some destination *D*. Detecting the broken link is the responsibility of each node along the route. When the node has packet to transmit to the next hop detects whether its link to the next hop has broken or not.

Route breaks could occur due to node mobility, fading environment, signal interference, and packet collisions. Link breakage can be detected if a node receives a link layer feedback signal from the wireless MAC protocol such as IEEE 802.11 [44], where the MAC protocol retransmits each packet until a link-layer acknowledgment is received, or until a maximum number of transmission attempts have been made. Alternatively, in HARP1, link breakage detection and a route error message are raised when one of the following steps occurs:

1. If T_d is expired at intermediate node during route request, an Error message of type "*Time* T_d *expire*" will be backtracked to the original sender S along the *LRR* being built along the route request path.
2. If T_n (T_n is a time set by a node to find its neighbours) is expired and the intermediate node cannot hear or find any neighbour, an Error message of type "*Time* T_n *expire*" will be sent to the upstream node to perform axis mapping along different heading direction (Local Repair) to overcome the broken link and find an alternative link.
3. At a broken route (at route reply and sending data), if a downstream node cannot find the upstream neighbour that has a record in *LRR*, an error message of type "*Broken Route*" is prepared. This error message then sent to previous downstream node (Local Repair) to perform axis mapping, and to find new neighbour to propagate the message in direction of an upstream node of *LRR*.

There are two methods to handle a broken route. When the detecting node returns a route error packet to the original sender *S* of the packet, the sender *S* can then attempt to use any other route to *D* that is already in its route cache or can invoke route discovery again to find a new route for subsequent packets. The former method is used when S has a valid path to the destination (valid path is the path that is used recently and not expired or the path that recently established and not expired yet). Otherwise, the latter method is used.

4.3 Simulation Methodology and Model

In fact, most scenarios (the behaviour of nodes in the real world is not known) used in mobile ad hoc networks are still unknown. This is due to two main reasons, the first reason is the difficulty of predicting the dynamic behaviour of mobile ad hoc networks.

The second reason is that ad hoc networks are still mainly a research subject. Therefore, the real life measurements are difficult and costly. Hence, simulation is a tool used for comparing ad hoc routing protocols. Tarek Helmi Abd El-Nabi [97] explained this by saying: "*There are three different ways to model networks: formal analysis, real life measurements and simulation [98]. The dynamic nature of ad hoc networks makes them hard to study by formal analysis. Some formal techniques that have been used in static networks include Petri nets, stochastic processes, queuing theory, and graph theory. None of these is especially well suited to studying dynamic networks. Since ad hoc networks are still mainly a research subject, most scenarios they will be used in are still unknown. For those scenarios that are known, e.g. military networks, extreme uncertainties and dynamicity are expected. Thus, use of real life measurements is currently almost impossible and certainly costly. The commonly used alternative is study the behaviour of the protocols in a simulated environment*".

In addition, by using simulation, it is possible to evaluate and test the behaviour of networks with a longer number of mobile nodes and different sizes of network area than physical devices are available for or fixed area. Moreover, it allows near perfect experimental control by testing the protocols for different parameters values then rerunning while varying an experimental variable and holding all other variables constant.

Many researchers in MANET have evaluated and simulated their works using different approaches and simulation tools. The most popular network simulators are: the Network Simulator NS-2 [99, 100], Global Mobile Information System Simulation Library GloMoSim [101], and OPNET Modeler [102], some works has been simulated by using one of the Programming languages as C, C++, and Java [75, 103].

4.3.1 Simulation Environment

In this section, the performance of HARP1 routing protocol is evaluated by simulation. The Network Simulator NS-2 is used to perform extensive simulations and to evaluate HARP1 protocol. What distinguishes NS-2 [99, 100] from other simulators is the range of features it provides and been an open source code that can be modified and extended. NS-2 is a discrete event and an object-oriented simulator targeted at networking research and developed by the University of California at Berkeley and the VINT project [104]. There are several different versions of NS-2 and at the current time, the latest version is NS-2.29. NS-2 provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless networks.

NS-2 is written in C++, with an OTcl (Object Tool Command Language) interpreter as a command and configuration interface. The C++ part, which is fast to run but slower to change, is used for detailed protocol implementation. The OTcl part, on the other hand, which runs much slower, but can be changed very quickly, is used for simulation configuration. One of the advantages of this split-language programming approach is that it allows for fast generation of large scenarios. One of the key hurdles to advancing MANET technologies from single-tier, 2-D topology to multi-tier, 3-D topology is the lack of research tools that support 3-D simulation and visualization [105]. For example, the wireless Extension of NS-2 and NAM (Network AniMator) [89], which have been among the most popular MANET research tools is short of 3-D support. Ryu et al. [105] present a 3-D extension of NS-2 and NAM for mobile ad hoc network.

4.3.2 Parameter Values

In the simulation model, the number of mobile nodes is ranges from 10 to 70 mobile hosts placed randomly within the simulation area. Each simulation has been executed for 500 seconds of simulation time. The network space for each simulation was chosen as 1km x 1km. The square site models situations in which nodes can move freely around each other, and where there is a small amount of path and spatial diversity available for the routing protocol to discover and use. The network traffic was modelled as 10 Constant Bit Rate (CBR) sources. All communication patterns were peer-to-peer, and connections were started at times uniformly distributed between 0 and 180 seconds (the maximum value allowed in NS-2). The reason of not using TCP sources in the simulation is because of the behaviour of TCP in offering a conforming load to the network by changing the times at which it sends packets based on its perception of the network's ability to carry packets. As a result, both the time at which each data packet is originated by its sender and the position of the node when sending the packet would differ between the protocols, preventing a direct comparison between them.

In terms of mobility model, a Random WayPoint Model (RWP) [106] is used for different values of pause time, max node speed, and network size. The random waypoint model is one of the most widely used mobility models in performance analysis of mobile wireless networks.

The IEEE 802.11 Medium Access Control (MAC) Distributed Coordination Function (DCF) [44] protocol is used in the simulation to get the link breakage feedback signal. The physical radio characteristics of each mobile node's network interface, such as the antenna type, transmit power, and receiver sensitivity, were chosen to approximate the most common commercially wireless LAN radio such as Lucent WaveLAN [90] radio. Radio propagation range for each node was 250 meters and channel capacity was 2 Mbps. The propagation model used in the simulation combines both a free space propagation model and a two-ray ground reflection model. The size of data payload generated by the source node was chosen to be 512 bytes in all the simulation scenarios. Using more than 512 bytes such as 1024-byte, packets will result in congestion, due to lack of spatial diversity. This congestion will become a problem for the algorithms and some nodes would drop most of the packets that they received for forwarding. Table 4-1 provides a summary of the rest of the simulation parameters.

The results presented are mean values of multiple runs for each scenario and collected data was averaged over those runs. For fair comparisons, the same set of mobility and traffic scenarios are used in all simulated routing HARP1 and AODV protocol.

Table 4-1: Parameters of simulation
Used with NS-2 and Random Waypoint

Scenario Name	*Pause Time Scenario*	*Max Node Speed Scenario*	*Network Size Scenario*
Pause time (s)	0,50,100,200, 300,500	10	10
Max Node Speed (m/s)	10	10,20,30,40,50,60	10
Number of mobile nodes	50	50	10,30,50,60,70
Simulation Time (s)	500	500	500
Network Space	1kmX1km	1kmX1km	1kmX1km
Radio range	250m	250m	250m
MAC Protocol	IEEE 802.11	IEEE 802.11	IEEE 802.11
Radio propagation model	Free space/ two-ray	Free space/ two-ray	Free space/ two-ray
antenna model	Omni Antenna	Omni Antenna	Omni Antenna
Traffic pattern	CBR	CBR	CBR
Maximum number of connections	10	10	10

4.4 Simulation Results and Analysis

This section consists of two main parts, the performance metrics used for evaluating the performance of the HARP1 routing protocol, and the results extracted from the simulation with the analysis of these results.

4.4.1 Performance Metrics

The following performance metrics are used for comparisons:

The route discovery packets (the Overhead) are defined as the number of all control packets generated by all nodes in the network in order to establish routes between sources and destinations.

The efficiency of data packet delivery is defined as the measured ratio of the number of data packets delivered to the destinations to the number of all packets generated in the networks. Note that each time a packet is forwarded, it is counted as one packet transmission. This metric is used to investigate how efficiently control packets and the selection of long-lived routes are utilised in delivering data packets.

The average end-to-end delay of transferred data packets includes all possible delays caused by buffering during route discovery, queuing at the interface-queue, retransmission delays at the medium access control layer, propagation and transfer times, and ARP delay that has a considerable value especially in the second scheme where eight packets need to be sent and need some delay between them.

Each metric parameter mentioned above has been simulated in three different scenarios:

1) Mobility scenario: with different pause time values,
2) Speed scenario: with different node speeds,
3) Network sizes scenario: with different number of nodes.

A comparison of the HARP1 with AODV has been made

4.4.2 Results and Analysis

The solid lines in Figures 4-2, 4-3 and 4-4 show an appropriate line of best fit to the experimental data. Figures 4-2, 4-3, and 4-4 show the route discovery packets against mobility with different pause time, maxima of node speeds, and network size respectively. It can be seen in HARP1 that the route discovery packets needed to find the path are much less than the packets needed in AODV protocol. Regarding to pause time, the average route discovery packet is about 13730, while in AODV is about 153213. In addition, as speed increases, the number of route discovery packets of the HARP1 remains nearly steady; in contrast to AODV where the number of these packets increases rapidly. It can be seen in Figure 4-4, that as the number of nodes increases, the number of route discovery packets slightly increases. This means that the HARP1 scales well with the network size in terms of overhead cost.

The route discovery packets in HARP1 are the less affected by mobility, node speed and network size due to the fact that in all situations the node will select only one neighbour to forward packets to. The AODV routing protocol floods the request packet to all nodes across the network. This leads to a greater number of route discovery packets as shown in figure 4-2. Whilst in HARP1 and in all scenario, the node selects only one nodes to transmit the request packet, therefore the route discovery remains steady along the simulation time.

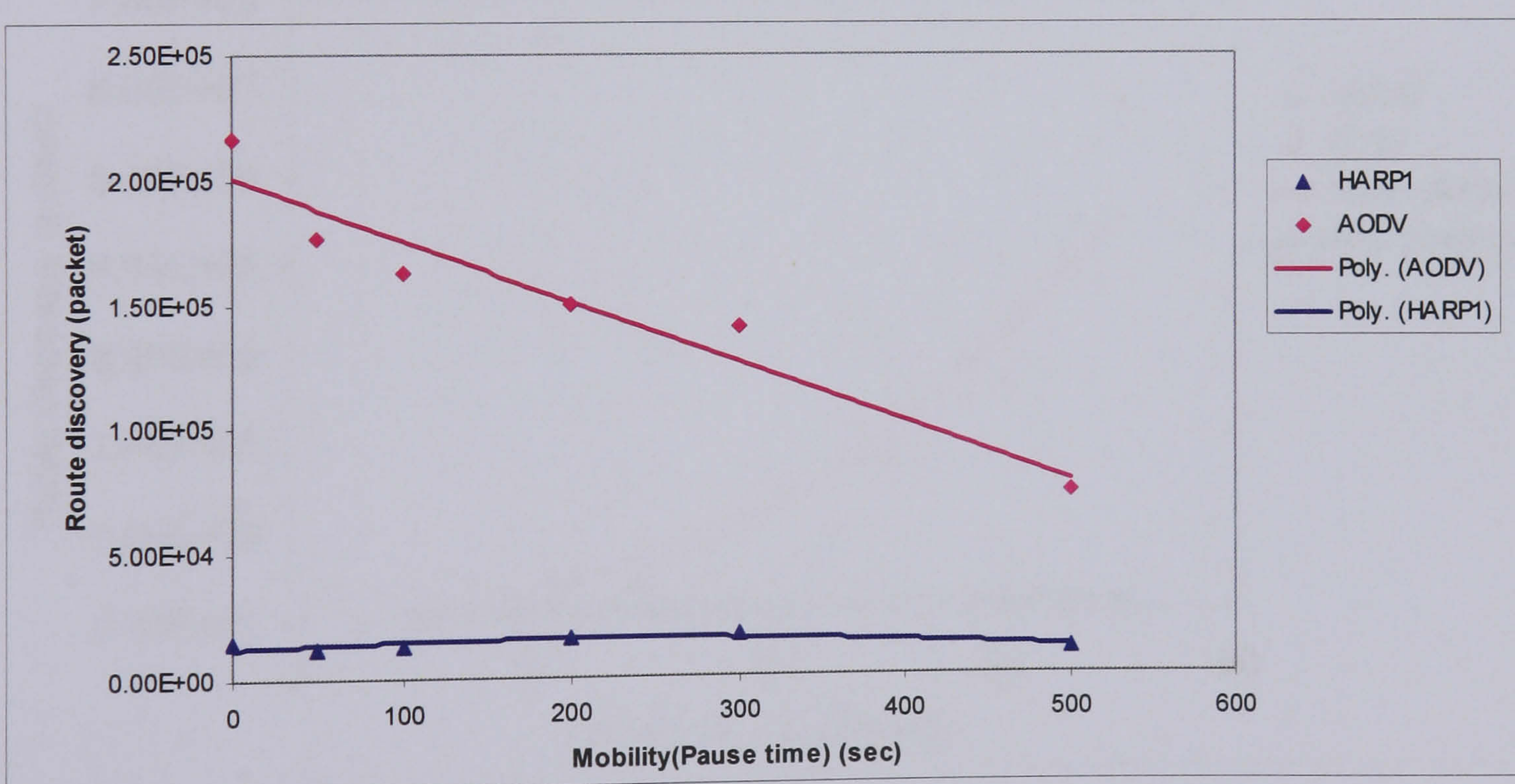


Figure 4-2: Route Discovery vs. Mobility (Pause Time)

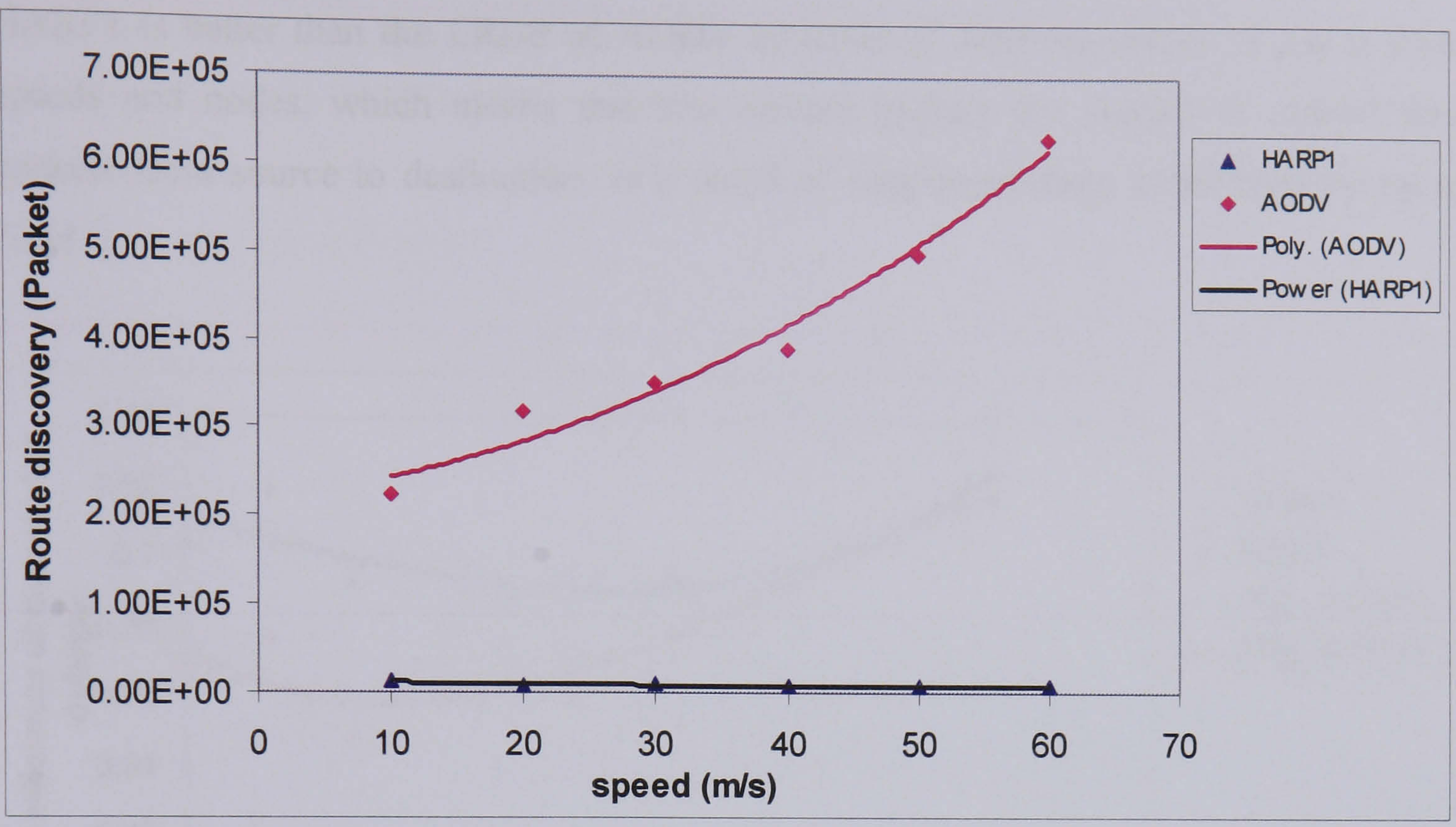


Figure 4-3: Route Discovery vs. speed

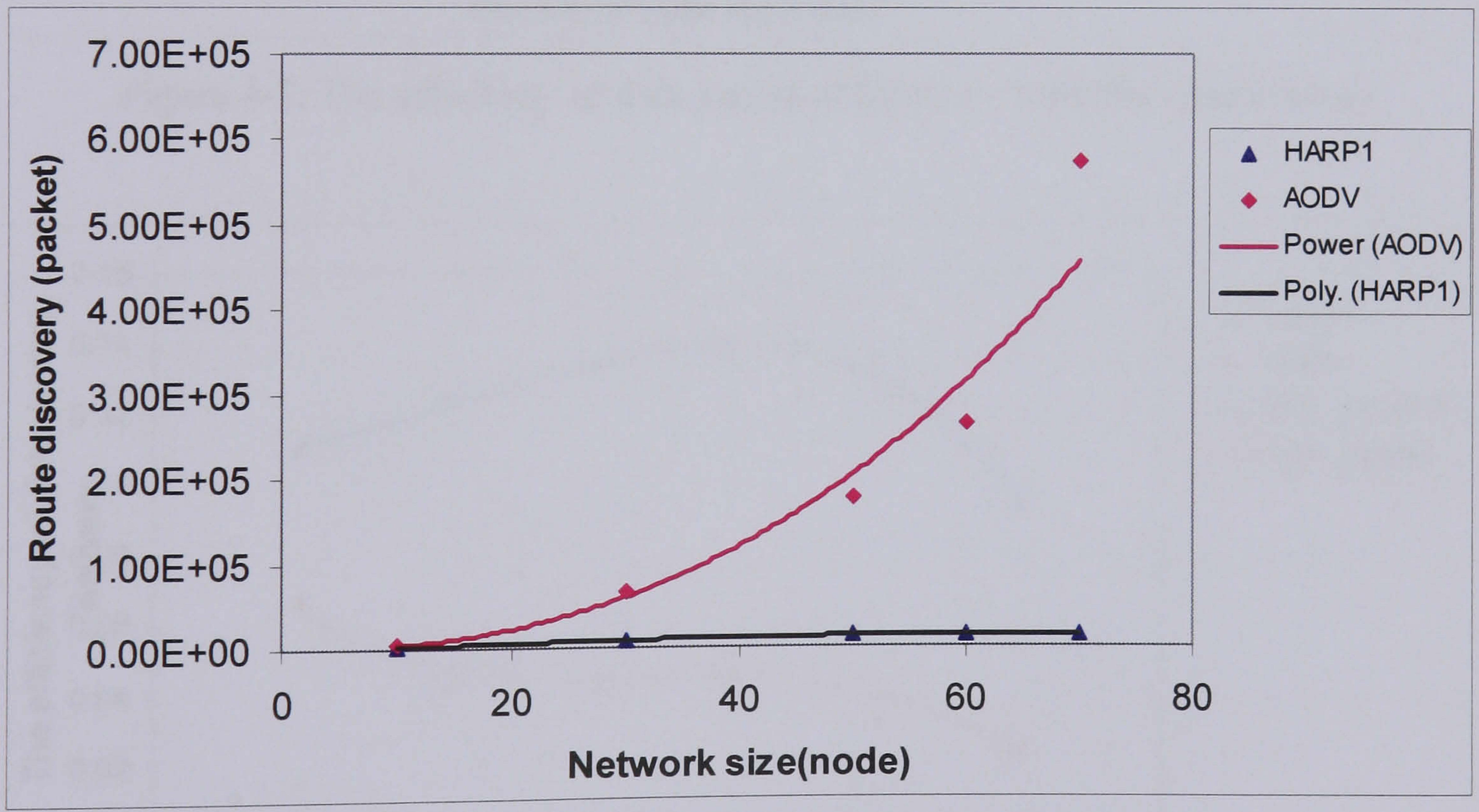


Figure 4-4: Route Discovery vs. Network size

Figures 4-5, 4-6 and 4-7 show the Efficiency Ratio of Data Packet delivery (ERDP) against mobility with different pause time, maxima of node speeds, and network size. Higher ERDP means better performance. As can be seen in these figures, ERDP in the

HARP1 is better than the ERDP of AODV in terms of different values of pause time, speeds and nodes, which means that less control packets are needed to deliver data packets from source to destination, as a result of long-lived route established by using *HDA*.

Figure 4-5: The efficiency of data packet delivery vs. Mobility (pause time)

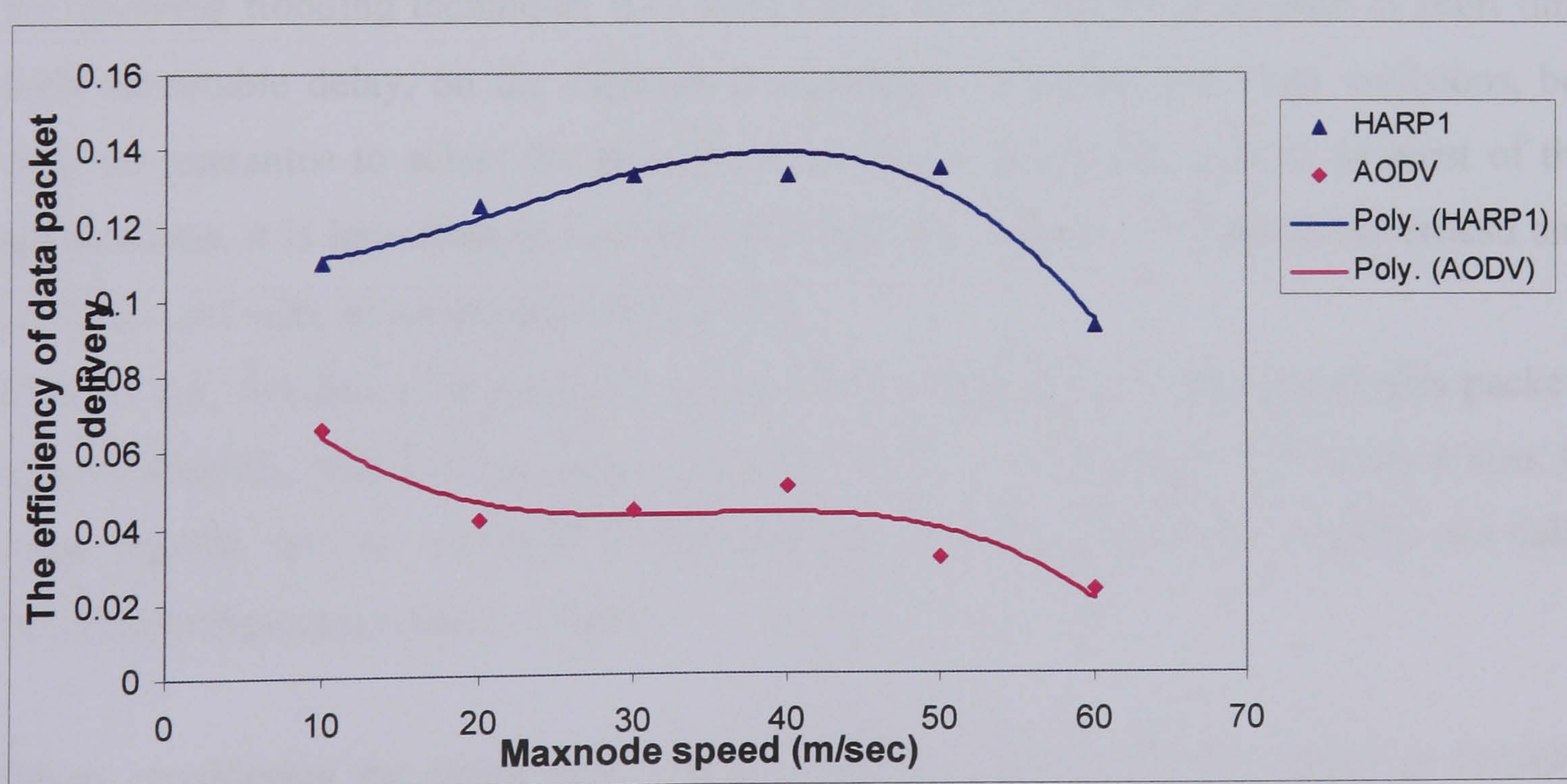


Figure 4-6: The efficiency of data packet delivery vs. speed

It can be seen from Figure 4-7, when the number of nodes is in the range [10-40], the ERDP of HARP1 is decreasing but when the number of nodes is greater than 40, the

ERDP increases. This leads to the conclusion that when there are more nodes in an ad hoc network, a greater number of nodes will contribute in the formation of the route, which cause a decrease in the probability of link breaks and thus, a smaller number of data packets being delivered.

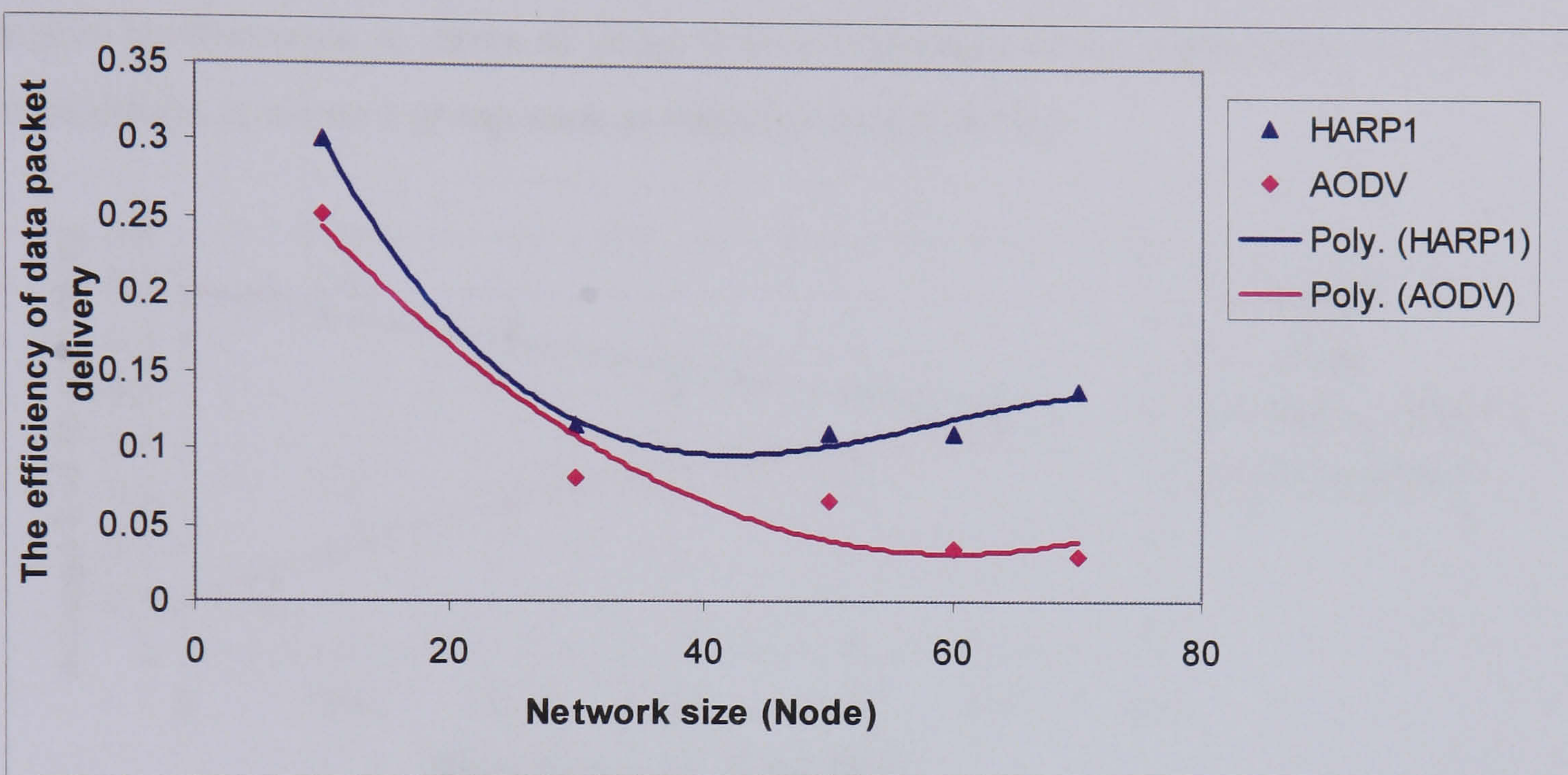


Figure 4-7: The efficiency of data packet delivery vs. Network size

By applying flooding technique, it is most likely to find the required path in short time with acceptable delay, on the expense of significant overhead and more collisions, but with no guarantee to select the path that lasts for an acceptable period. In most of the applications, it is important to find the path that lasts longest with reduced overhead and collision and with an acceptable level of delay.

Figures 4-8, 4-9 and 4-10 show the average end-to-end delay of transferred data packets against mobility with different pause time, maxima of nodes speeds, and network size. In these figures, we can see that HARP1 has an increased delay compared to the fully flooding technique protocol, AODV.

When considering the pause time (Figure 4-8), the delay is mostly steady in HARP1 although when the speed of nodes is increased, the average end-to-end delay is gradually decreased. This is because there are more neighbours with near heading directions angle to the upstream node to choose from as downstream node. When the number of nodes is increased, the average end-to-end delay is increased as well due to the increased number of nodes that form the route, which also lead to more frequent breaks.

If HARP1 is implemented as a stand-alone protocol instead of implementing it in other existing protocols in order to improve their performance then this scheme achieves much higher performance in terms of delay if it is implemented for applications in which the nodes/users move as a group such as vehicles on a highway.

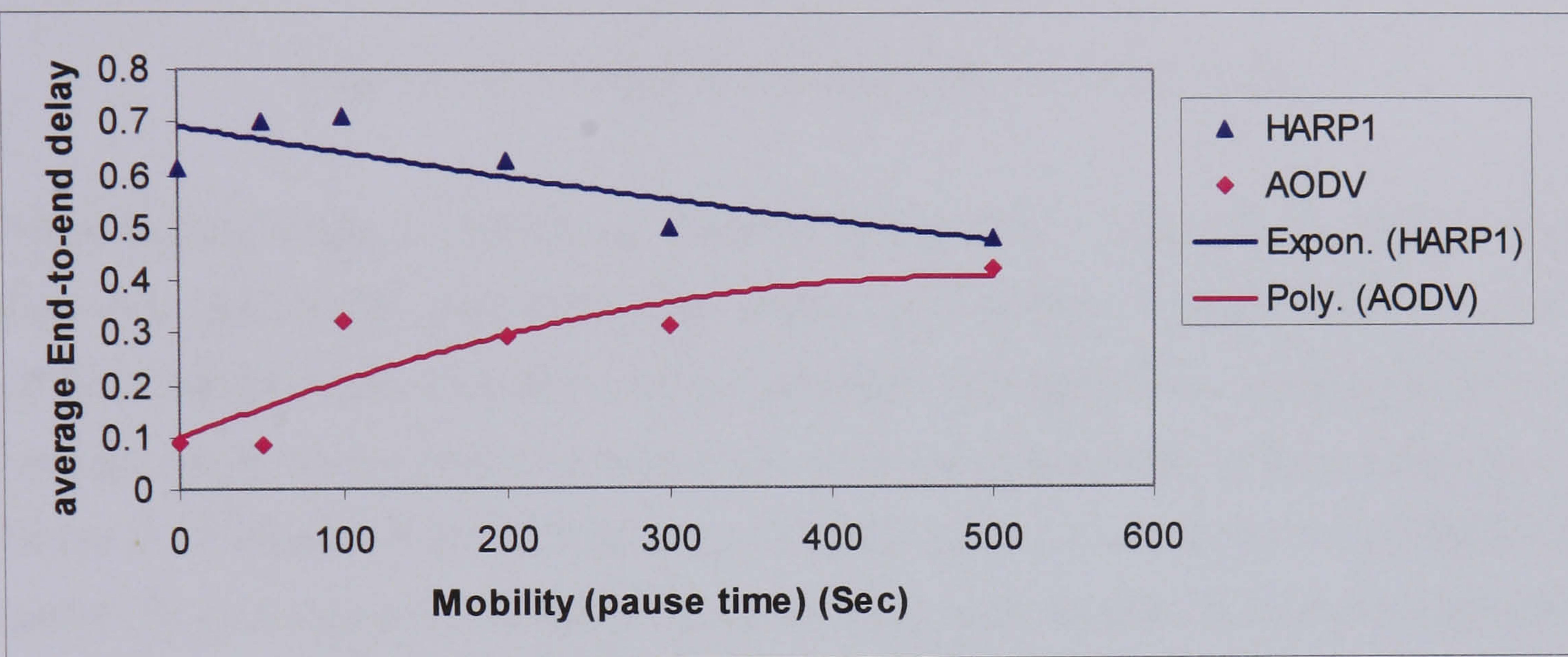


Figure 4-8: Average End-to-end delay vs. Mobility (pause time)

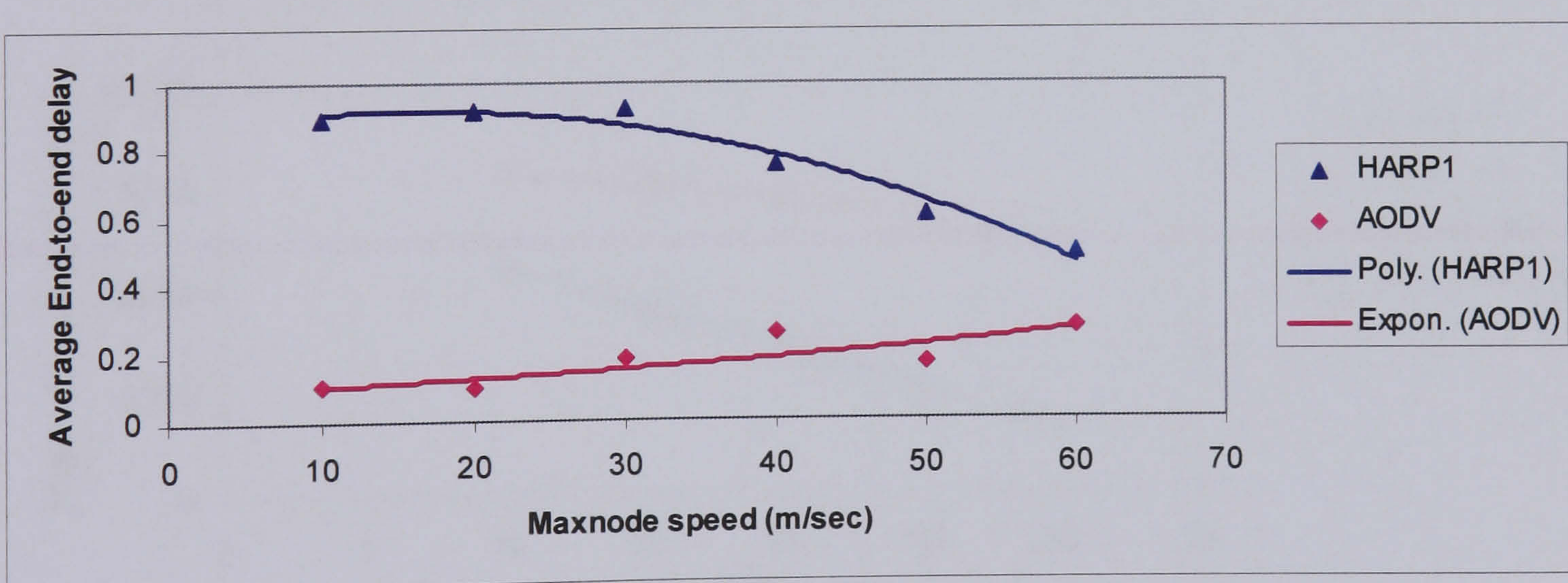


Figure 4-9: Average End-to-end delay vs. speed

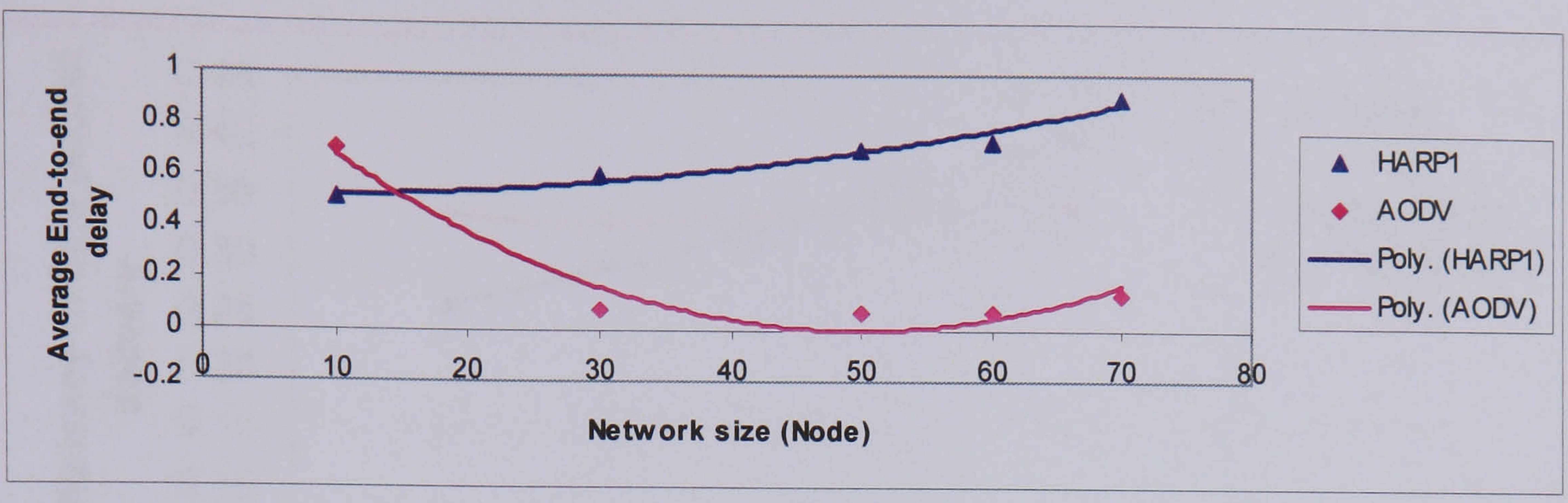


Figure 4-10: Average End-to-end delay vs. Network size

When looking at group mobility, as depicted in Figure 4-11 it can be seen that the route discovery packets with maxima of node speeds for HARP1 is suitable. It can be seen in HARP1 that the route discovery packets needed to find the path are much fewer than the packets needed in the AODV protocol and the number decreased with increased speed. Figure 4-12 shows ERDP with maxima of node speeds. It can be seen that ERDP for HARP1 is increased with increased speed, since a greater number of choices for selecting the next downstream node is available in the group mobility scenario.

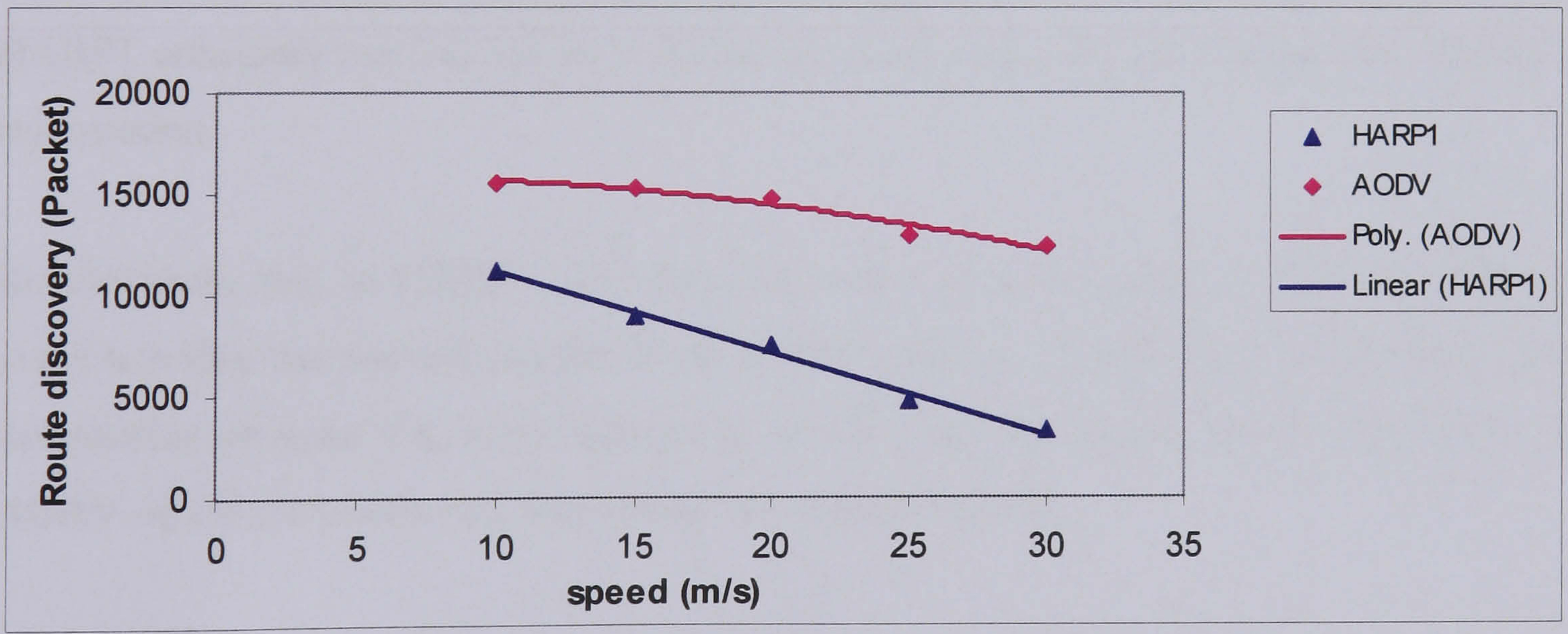


Figure 4-11: Group mobility. Route Discovery vs. speed

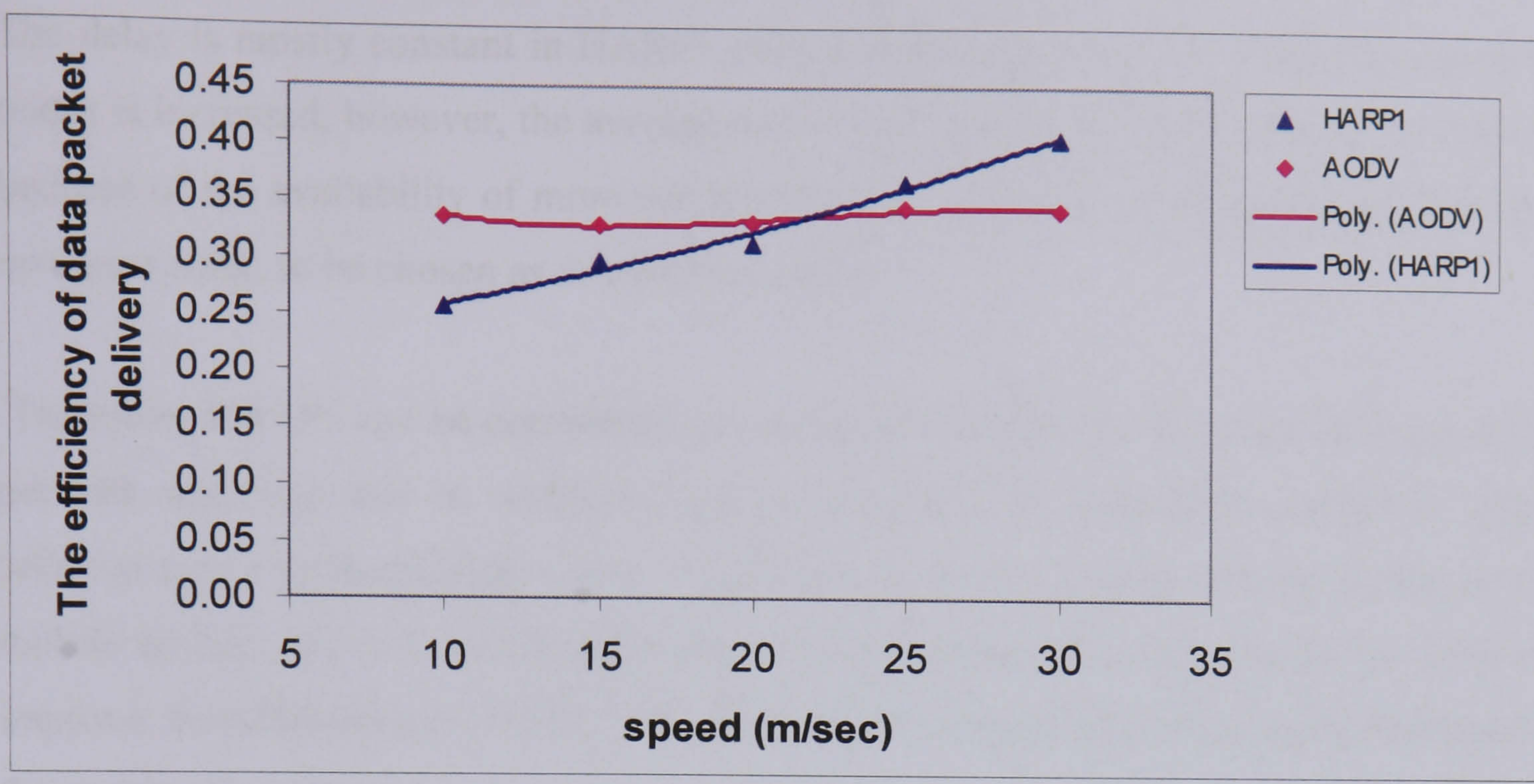


Figure 4-12: Group mobility. The efficiency of data packet delivery vs. speed

4.5 Summary

In the proposed algorithm (HARP1), the use of HDA of nodes to select the most robust and long-lived link between each two communicating nodes is investigated. In addition, HARP1 considers that the ad hoc network is short of any external resources of routing information.

Results show that in HARP1, the route discovery packets needed to find the path are much less than the packets needed in the AODV protocol. In addition, as speed increases, the number of route discovery packets of HARP1 remains nearly steady; in contrast to AODV where the number of these packets increases rapidly.

HARP1 scales well with the network size in terms of overhead cost, although the number of route discovery packets slightly increases when the number of nodes increases. The ERDP in HARP1 is better than the ERDP of AODV in terms of different values of mobility, speeds and nodes meaning that fewer control packets are needed to deliver data packets from source to destination as a result of long-lived route established by using *HDA*.

The delay is mostly constant in HARP1 with a different pause time. When the speed of nodes is increased, however, the average end-to-end delay is gradually decreased. This is because of the availability of more neighbours with near heading directions angle to the upstream node, to be chosen as downstream node.

Therefore, HARP1 can be considered as a solution to handle the frequent changes in the network topology due to mobility; and to maintain the long-lived multi-hop paths between two communicating nodes. Consequently, other existing routing protocols for mobile ad hoc networks could apply the technique proposed in this chapter in order to improve the performance or QoS of these protocols in terms of elongating the lifetime of the communications.

Chapter 5

HARP2 (Heading-Direction-Based Routing Protocol)

In this chapter, a novel routing approach for multiple-hop mobile ad hoc networks is presented. HARP1 protocol has been explained in chapter 4 which can operate in stand-alone mode (another possible mode is to be implemented in other existing protocols). In this mode, the chance of finding the destination from the first attempt of route discovery is low due to only selecting one neighbour from only one zone-direction in each attempt. Therefore, to increase the efficiency of HARP1 protocol by increasing the probability of finding the destination with minimum number of tries, HARP2 is proposed.

When a link between two communicated nodes that is in operation is disconnected, the task of the routing protocol is to adapt to the new situation. This creates a cost that affects the overall performance of the network. The costs will be in the amount of control traffic and in the message delay. Thus, the more perdurable links are better for data transmission than the less perdurable links.

Another motivation of designing and proposing HARP2 is the need for a mechanism that reduces the amount of control messages (overhead) used for establishing a route between two communication nodes.

HARP2 protocol for mobile ad hoc networks is also proposed with the aim of achieving efficient routing and reducing the effect of mobility.

5.1 HARP2 Routing Protocol

In this chapter, the operation of the second proposed Heading-direction Angle Routing Protocol (HARP2) is presented. HARP2 is, again, based on reactive on-demand philosophy. The HARP2 operation, the same as HARP1, can be considered as two parts: the first part is the mobility and nodes classification, whilst the second part is the route construction. The second part consists of route discovery and route maintenance.

5.1.1 Mobility and Nodes Classification

This part has been explained in detail in chapter three. In a few words, the HARP2 protocol considers that each mobile node in the ad hoc network sends its mobility information to its neighbouring nodes periodically. According to the received information the mobile node in the network is able to group its neighbouring nodes according to their heading directions into eight different zone-direction groups (z_1, z_2 ... z_8), as each mobile node divides the heading directions into different sectors.

5.1.2 Route Discovery

In HARP2, as with other on-demand routing algorithms, the principle of constructing a route between source and destination nodes relies on route discovery and route maintenance techniques. In HARP2, unlike other existing on-demand algorithms, the operations of route discovery at the source node are different from the operations at intermediate nodes.

5.1.2.1 Route Discovery at the Source Node

Discovering the route in HARP2 starts from the source node that has data packets for an intended destination. At the source node *S*, when *S* has data packets to send to a specific destination node *D*, *S* will request a route to that destination *D*. Firstly, *S* will look in its cache memory for the destination. If the destination is available in the cache memory, *S* will start forwarding the data packets to the destination. If *D* is not available in the source's cache memory, a time T_d will be set up by *S*, where T_d is the time required to find *D*. Then, *S* will select one neighbour from each zone from the eight different zone-direction groups (z1, z2 ... z8) of neighbours. Therefore, at most eight neighbours will be selected in the same time as shown in Figure 5-1.

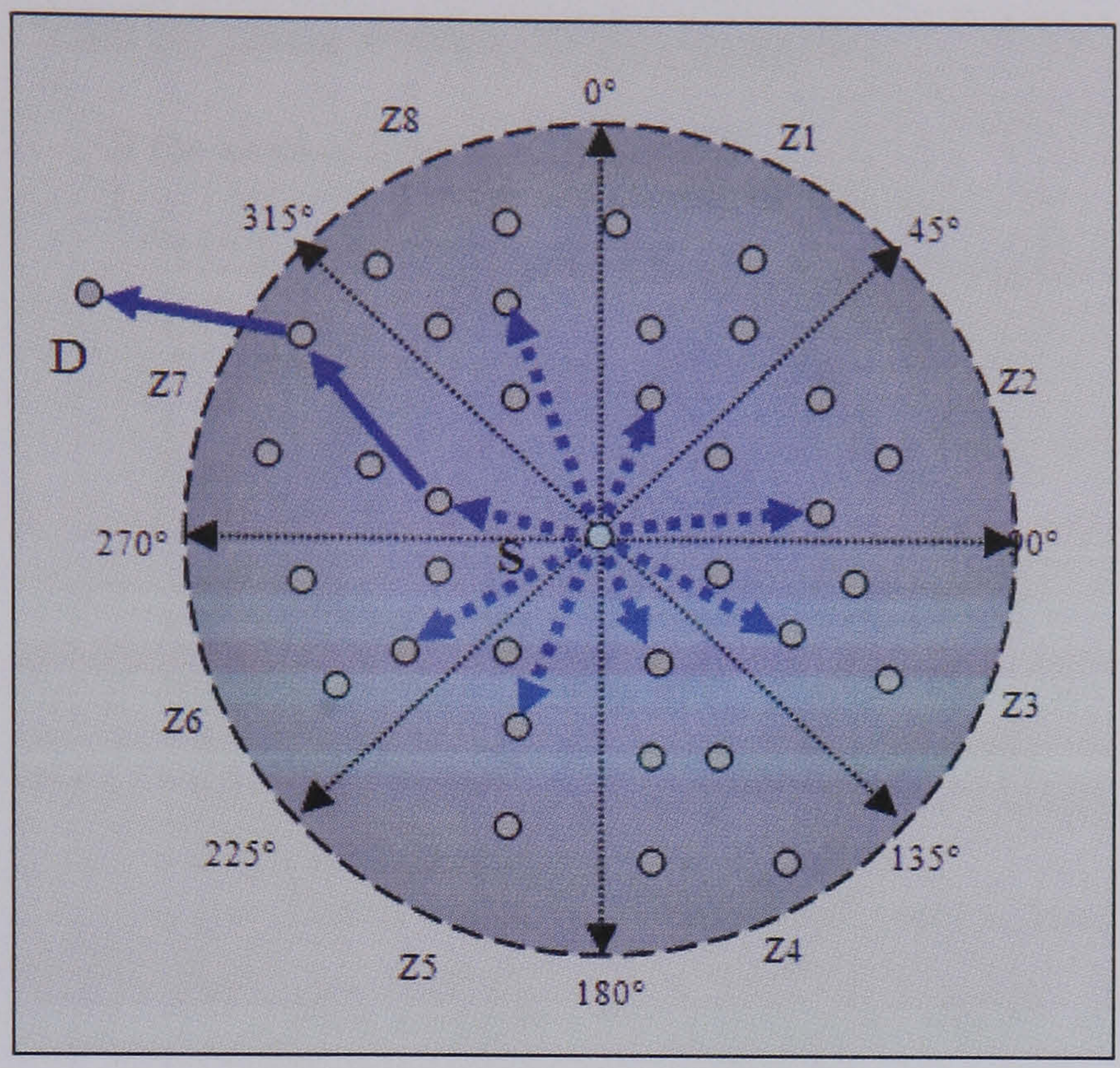


Figure 5-1: The source S selects one neighbour from each zone to send a request packet

A LRR is then initiated as described in HARP1,where a new record is added containing information about the source node (A node IP address, a node heading angle, and a zone-direction number). After, the route request message that includes the *LRR* will be propagated to all the selected neighbours.

If a neighbour in one zone-direction of *S'* direction zones is not available, the number of selected neighbours will be less than eight. All the nodes that receive the route request will update their route cache entries by updating the information of the node (as a neighbour) from which the message was received. Only the intermediate node that the message is addressed to will accept the message. Other nodes will silently drop this message. Figure 5-2 shows the pseudo-code algorithm that is running at the source node.

```
If RREQ_Count <= Max_RREQ_Count then
{
   If the node is S then
   {
     If IPAddr_D ∈ NbCache_S then        // if D is neighbour to S
     {
          Send (data packets to IPAddr_D);
     }
     Else
     {
       Init (T_d);                        // initiate T_d
       S_Dir = HDA of S;
       S_Zone = Zone number of S;
       Init (LRR); // initiate a List of Route Records
       //Add to LRR: S' Address, HDA of S, Zone number of S
       LRR_Add (IPAddr_S, S_Dir, S_Zone);
       For (ZoneNo = 1; ZoneNo<= MaxZoneNo; ZoneNo++)
       {
          // Find a neighbour in ZoneNo and skip the selected
          //neighbour in previous RREQ
          IPAddr_Nb = Find_Nb (ZoneNo);
          If IPAddr_Nb <> 0 then  // Neighbour is found
          {
             // Forward RREQ to a neighbour Nb
             Forward_RREQ (IPAddr_Nb)
          }
       }
     }
   }
}
Else STOP // do not initiate RREQ
```

Figure 5-2: Pseudo code for HARP2: RREQ at the source node *S* is addressed to the destination *D*

5.1.2.2 Route Discovery at the Intermediate/Relay Node

The intermediate node that the packet is addressed to will search in its cache memory of neighbours for the destination *D*. If *D* is found in the cache memory, the intermediate node will update the LRR by adding a record to it. This record contains information about the intermediate node itself. It then propagates a reply message along the nodes that have records in LRR. The LRR is backtracked to the initiating source node *S*. Whilst if *D* is not found in the cache memory as a neighbour, the same technique of finding a neighbour that has near heading direction to this node will be followed. Axis mapping technique will be followed for finding a suitable neighbour nearest in the direction to the intermediate node direction. Before forwarding the request packet to the next downstream node, the intermediate node will add a record to the LRR containing information about itself. If no neighbour is found for the time T_d, RREQ will be triggered again (S will repeat the route request a limited number of time e.g. 5 times in order to avoid the search-to-infinity).

In order to prevent loops in the search, the HARP2 algorithm uses a node's sequence number in addition to checking the availability of the selected neighbour node in *LRR* before sending the packet to that neighbour. If the neighbour is found in the list, another neighbour will be selected. At intermediate nodes, all the nodes that receive the route request message update their route cache entries by updating the information of the neighbouring node, from which the message was received. Only the intermediate nodes that the message is addressed to will accept the received route request message. Other nodes will silently drop it.

In HARP2, the path life between intermediate nodes will last longer because these nodes are selected to be near heading direction to each other. It is most likely that the route will be found from the first attempt due to forwarding the *RREQ* to eight neighbours in parallel manner. This proposed scheme is efficient in high-density networks, where the possibility of finding a neighbour in each zone is higher than in a low-density network. Instead of applying full flooding to all neighbouring nodes, the number of nodes that share in route discovery has been reduced to the number of direction zones at the source node (number of direction zones can be optimised according to the environment of the network and the application, in order to reduce the required time of finding the destination).

5.1.2.3 Route Reply

In HARP2, as in HARP1, when the addressed destination receives the route request packet, the destination will extract the *LRR* list that is carried in the route request packet. The destination will then piggyback the *LRR* list in the replied packet. The route reply packet will be sent by the destination along the reversed path mentioned in the *LRR* list.

In addition, a route reply packet is triggered by the intermediate node as well. When an intermediate node has received the route request packet, and has fresh routing information about the destination, the intermediate node will update the *LRR* list by adding its information. The *LRR* list is then piggybacked in the replied message. Finally, the intermediate node sends the reply message along the reversed path determined by the nodes recorded in the *LRR* list.

5.1.3 Route Maintenance and Local Repair

Route Maintenance, as mentioned in chapter four, is a mechanism used to detect the change in ad hoc network topology that leads to broken routes. As in all reactive routing approaches, detecting the broken link in HARP2 protocol is the responsibility of each node along the established route between the source and the destination nodes.

As in HARP1, in HARP2 the link is considered unavailable in three cases:

- When the time required to find the destination T_d is expired at an intermediate node during propagating the route request.
- When the time required by an intermediate node to find its neighbours T_n is expired, and this node cannot hear or find any neighbour. The intermediate node sends an error message of type "*Time* T_n *expire*" to upstream node. The upstream node performs axis mapping along different heading direction (Local Repair) to overcome the broken link and find an alternative link.
- The link is also considered unavailable when a downstream node cannot find the upstream neighbour that has a record in *LRR* during propagating a route reply message or data packets.

The source node that receives a route error message checks the number of attempts to establish the route to the destination. If the number of attempts is less than the maximum number of attempts allowed to find the destination, the sender *S* can then:

- Attempt to use any other route to the destination that is already available in its route cache.
- Alternatively, it can invoke route discovery again to find a new route for subsequent packets.

If the number of attempts is equal or greater than the maximum number of attempts, the sender application must consider the destination unavailable and should stop searching for it.

5.2 Simulation Model and Methodology

As mentioned in chapter 4, studying and investigating the way in which ad hoc networks behave in different environments and different parameters by a simulation are the commonly used method in mobile ad hoc networks.

5.2.1 Simulation Environment

The HARP2 routing protocol performance has been evaluated by simulation. The Network Simulator NS-2 was used to perform extensive simulations and to evaluate HARP2 protocol. In order to generate the movement of the mobile nodes, the CMU's scenario generating scripts have been studied to create these files and made use of the scenario-generation utility “setdest”. The node-movement generator is available under ~ns/indep-utils/cmu-scen-gen/setdest directory created when NS-2 is installed. The traffic-pattern file available with the ns distribution has also been used to generate the traffic patterns. This traffic generator script is available under ~ns/indep-utils/cmu-scen-gen directory in NS-2 Directory. This file is a TCL (Tool Command Language) script and named “cbrgen.tcl”.

5.2.2 Parameter Values

For simulating HARP2, and without loss of generality, the same parameter values used for simulating HARP1 were used, which will allow fair comparison between the two schemes. Table 5-1 provides a summary of the simulation parameters. The results presented are mean values of multiple runs for each scenario and collected data was averaged over those runs. For fair comparisons, the same environment, set of mobility, and traffic scenarios are used in all simulated HARP2 routing scheme and AODV protocol.

Table 5-1: Parameters values
Used with NS-2

Scenario Name	*Pause Time Scenario*	*Max Node Speed Scenario*	*Network Size Scenario*
Pause time (s)	0,50,100,200, 300,500	10	10
Max Node Speed (m/s)	10	10,20,30,40,50,60	10
Number of mobile nodes	50	50	10,30,50,60,70
Simulation Time (s)	500	500	500
Network Space (m)	1000 x 1000	1000 x 1000	1000 x 1000
Radio range	250m	250m	250m
MAC Protocol	IEEE 802.11	IEEE 802.11	IEEE 802.11
Radio propagation model	Free space/ two-ray	Free space/ two-ray	Free space/ two-ray
antenna model	Omni Antenna	Omni Antenna	Omni Antenna
Traffic pattern	CBR	CBR	CBR
Maximum number of connections	10	10	10

5.3 Simulation Results and Analysis

In this section, in addition to the analysis of results extracted from the simulation, the performance metrics used for evaluating the performance of HARP2 routing protocol is also presented.

5.3.1 Performance Metrics

As in HARP1, the following performance metrics are used for evaluating HARP2:

- ***The Route discovery packets (the Overhead)*** are defined as the number of all control packets generated by all nodes in the network in order to establish routes between sources and destinations.

- ***The efficiency of data packet delivery*** is defined as the measured ratio of the number of data packets delivered to the destinations to the number of all packets generated in the networks. Note that each time a packet is forwarded is counted as one packet transmission. This metric is used to investigate how efficiently control packets and the selection of long-lived routes are utilised in delivering data packets.

- ***The Average end-to-end delay*** of transferred data packets includes all possible delays caused by buffering during route discovery, queuing at the interface-queue, and retransmission delays at the medium access control layer. It also includes propagation and transfer times, and ARP delay that has a considerable value, especially in second scheme where eight packets need to be sent and need some delay between them.

Each parameter metric mentioned above was simulated in three different scenarios:

4) Mobility scenario: with different pause time values,
5) Speed scenario: with different node speeds,
6) Network size scenario: with different number of nodes.

5.3.2 Results and Analysis

Figure 5-3 shows the route discovery packets against mobility with different pause time (smaller pause time means higher mobility in the network). The solid lines in Figures 5-3, 5-4 and 5-5 show an appropriate line of best fit to the experimental data. It can be seen that with higher mobility (pause time between 0 and 50), HARP2 has a higher number of route discovery packets with a lower mobility (pause time greater that 50). As a result, a higher mobility require more packets to cope with the network topology change and route breaks recovery. In addition, it can be seen that the route discovery packets needed to find the path are much fewer in HARP2 than the route discovery packets needed in AODV protocol. This is due to the fact that the flooding technique used in AODV causes higher overhead control packet than the technique used in HARP2.

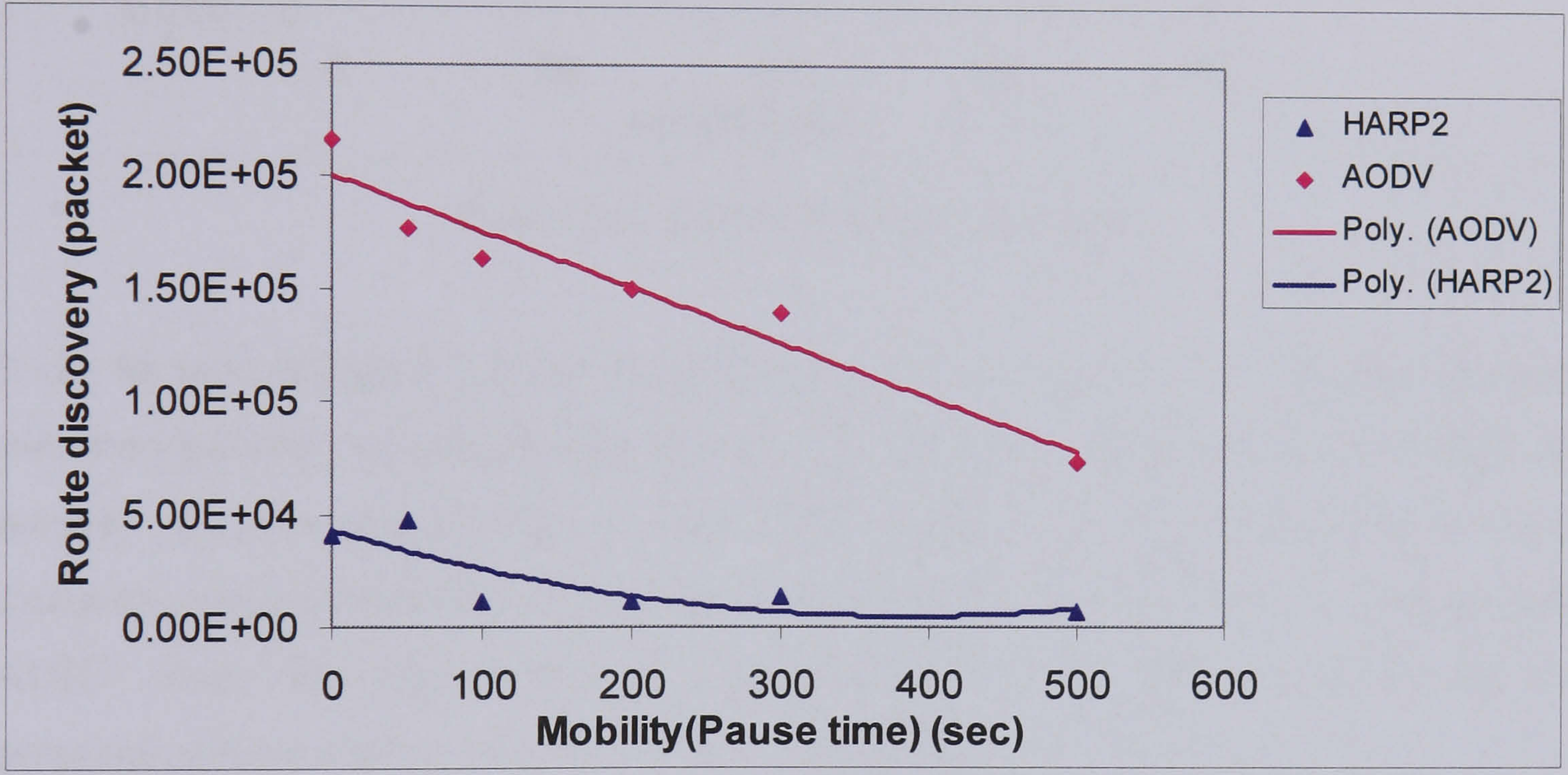


Figure 5-3: Route Discovery vs. Mobility (Pause Time)

Figure 5-4 shows the route discovery packets with different maxima of node speeds. It can be seen that for low speeds (< 20 m/s), the route discovery packets needed to find the path in HARP2 increase gradually. At maximum speed of 20 m/s and higher, the route discovery packets become nearly steady across the speed range from 20 to 60. In general, as can be seen in Figure 5-4, the route discovery packets required by HARP2 are much fewer than the packets needed in the AODV protocol across the speed range (from 10 to 60) as a result of good control and well distribution of route request packets. In addition, as speed increases, the number of route discovery packets generated by AODV increases rapidly due to the storm of flooding.

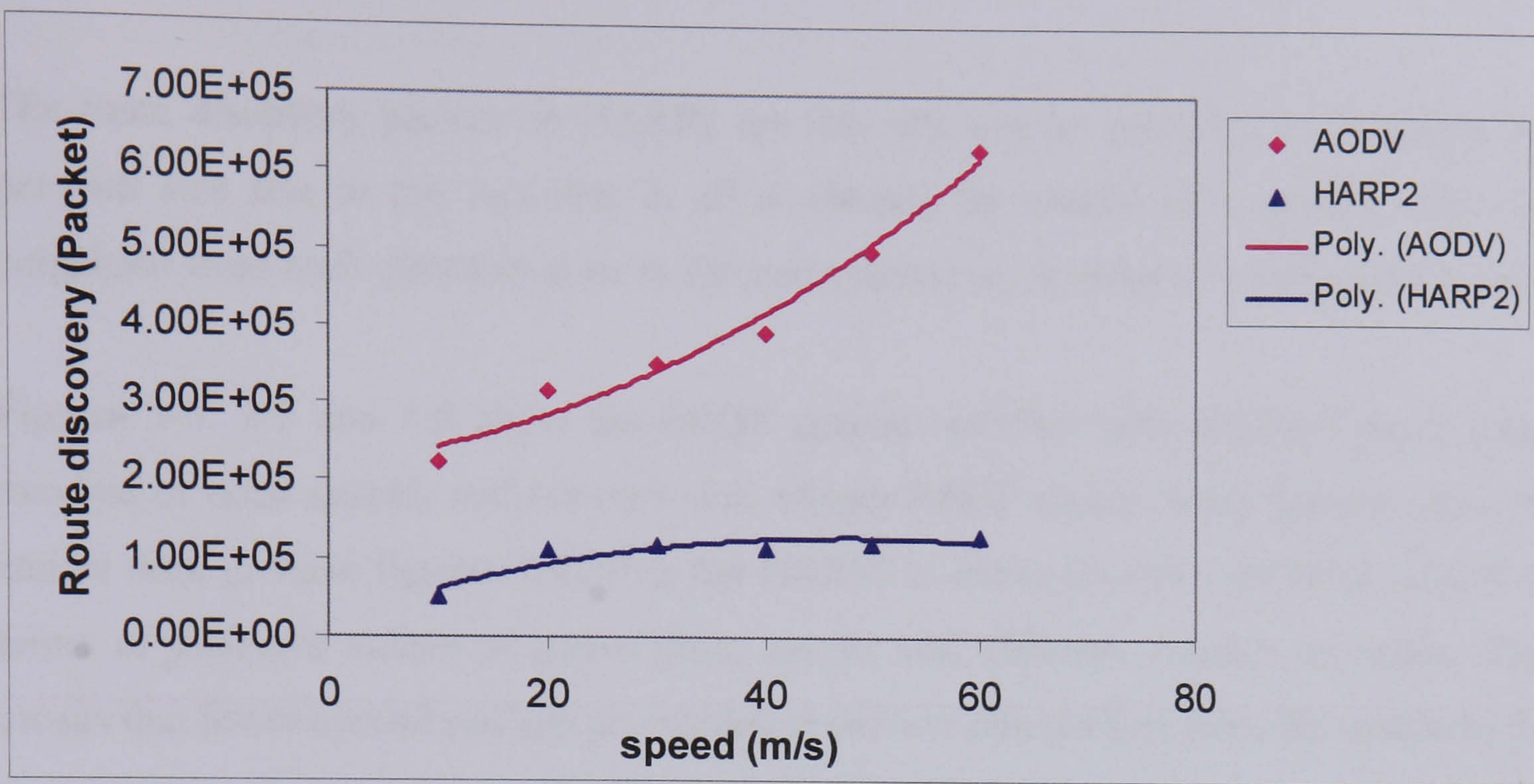


Figure 5-4: Route Discovery vs. speed

It can be seen in Figure 5-5 that as the number of nodes increases, the number of route discovery packets generated by HARP2 slightly increases compared with the AODV. At number of nodes greater than or equal to 60 (Node# >= 60), the number of route discovery packets required to find the path in HARP2 is roughly constant compared with AODV where this number increases sharply. This leads to the conclusion that the proposed scheme scales well with the network size in terms of overhead cost.

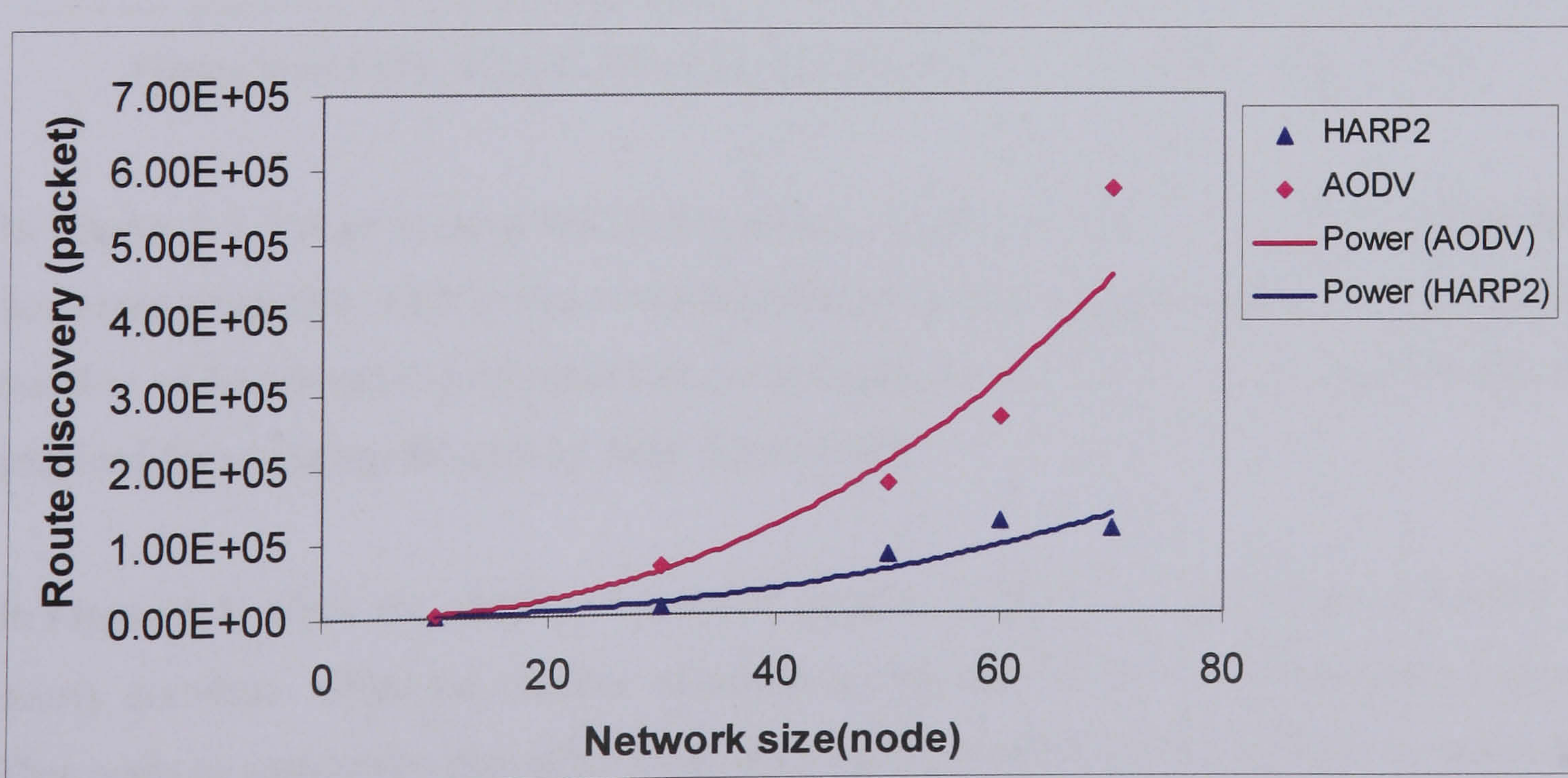


Figure 5-5: Route Discovery vs. Network size

The route discovery packets in HARP2 are less affected by mobility, node speed and network size due to the fact that in all situations, the source node selects only one neighbour from each direction-zone to forward packets to, in order to cover all directions.

Figures 5-6, 5-7 and 5-8 show the ERDP against mobility with different pause time, maxima of node speeds, and network size. Higher ERDP means better performance. As can be seen in these figures, ERDP in the HARP2 is better than the ERDP of AODV in terms of different values of pause time, speeds and different number of nodes. This means that fewer control packets are needed to deliver data packets from the source to the destination, as a result of long-lived route established by using HDA.

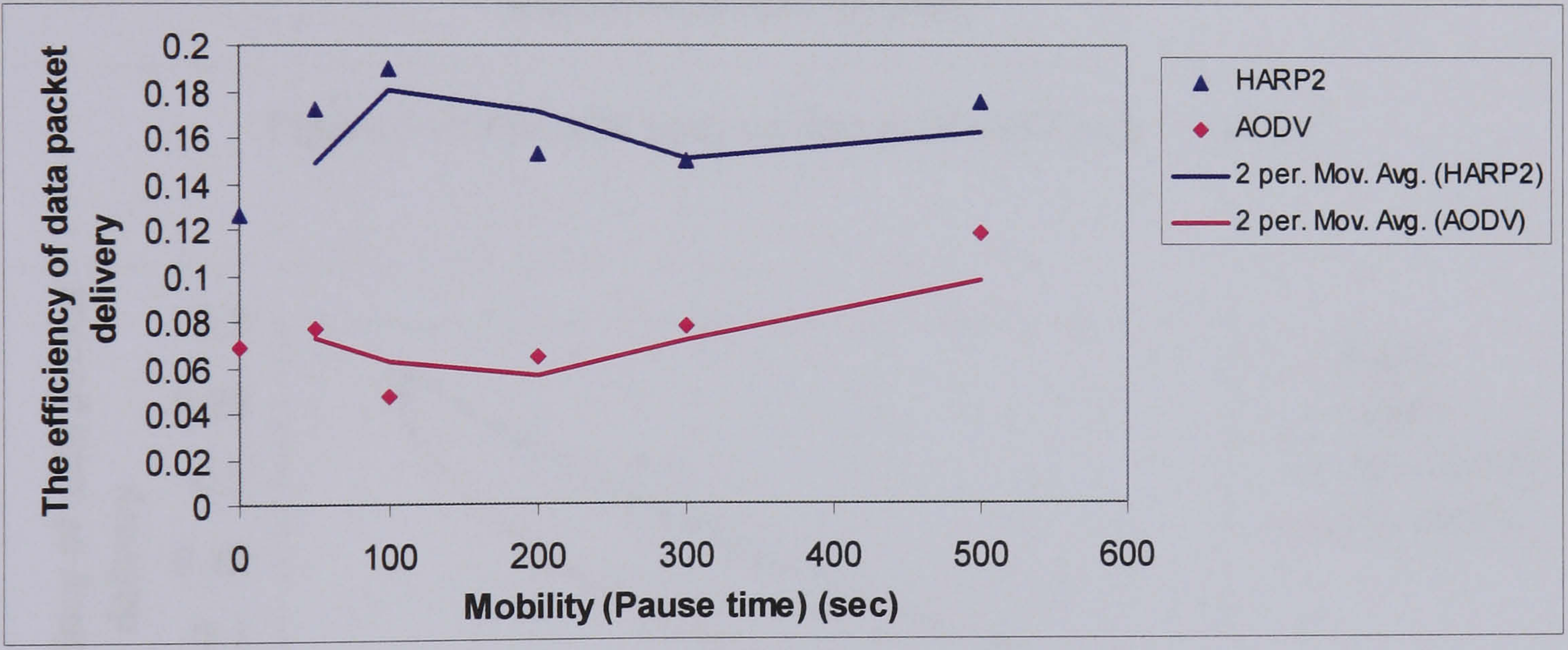


Figure 5-6: The efficiency of data packet delivery vs. Mobility (pause time)

In Figure 5-7, it can be seen that as the speed of nodes increases, the ERDP of HARP2 decreases gradually. This is due to the fact that when the speed of nodes is increased, the number of link breaks is increased as a consequence and, hence, the number of packets required for repairing the broken links is increased.

In Figure 5-8, when the number of nodes is equal to 50 and over, the ERDP of HARP2 is nearly constant. When the number of nodes is less than 50 the ERDP becomes higher. This leads to conclusion that when there are a higher number of nodes in ad hoc network, a higher number of nodes will contribute in the formation of the route. This leads to a higher probability of link breaks and thus, fewer number of data packets being delivered.

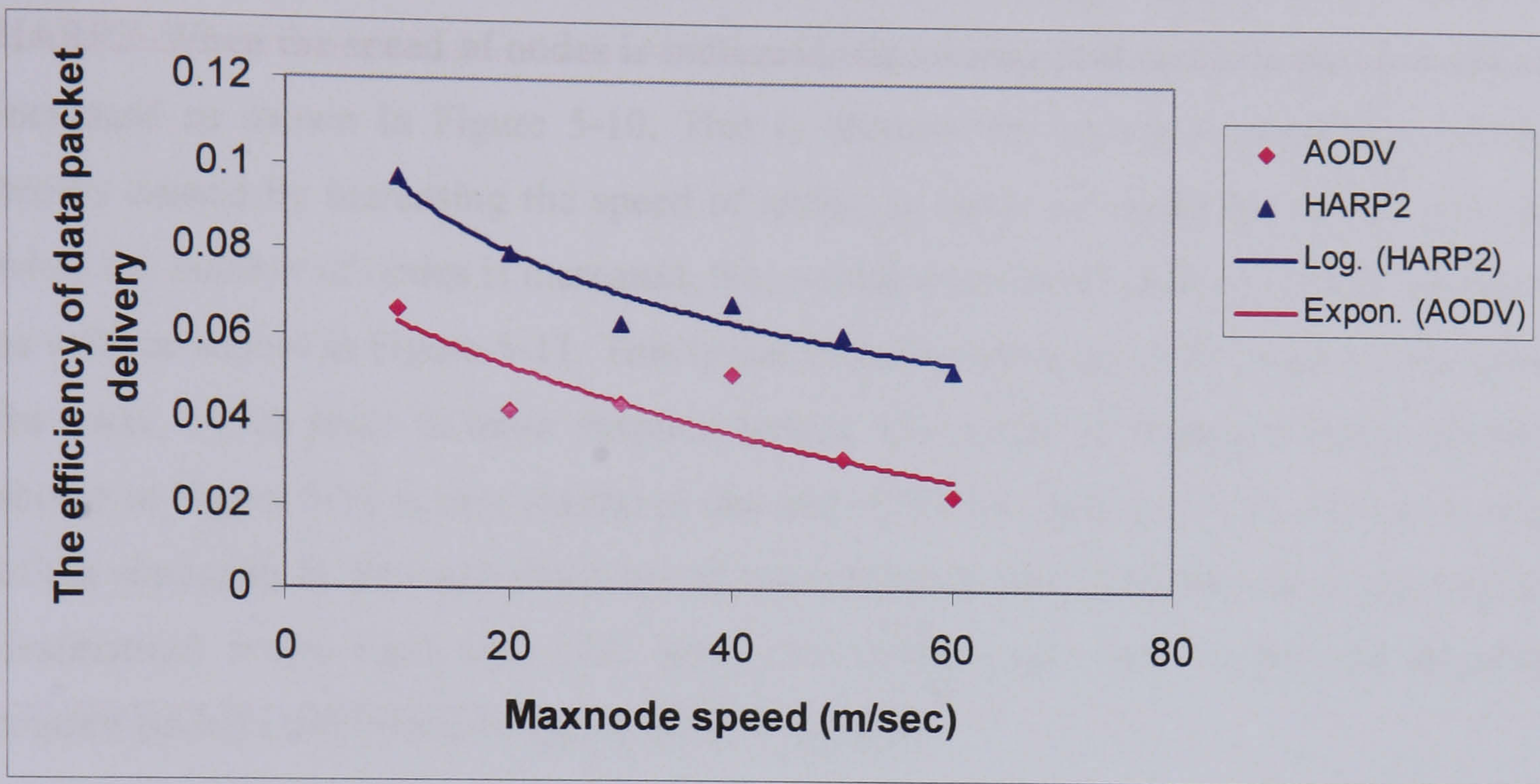


Figure 5-7: The efficiency of data packet delivery vs. speed

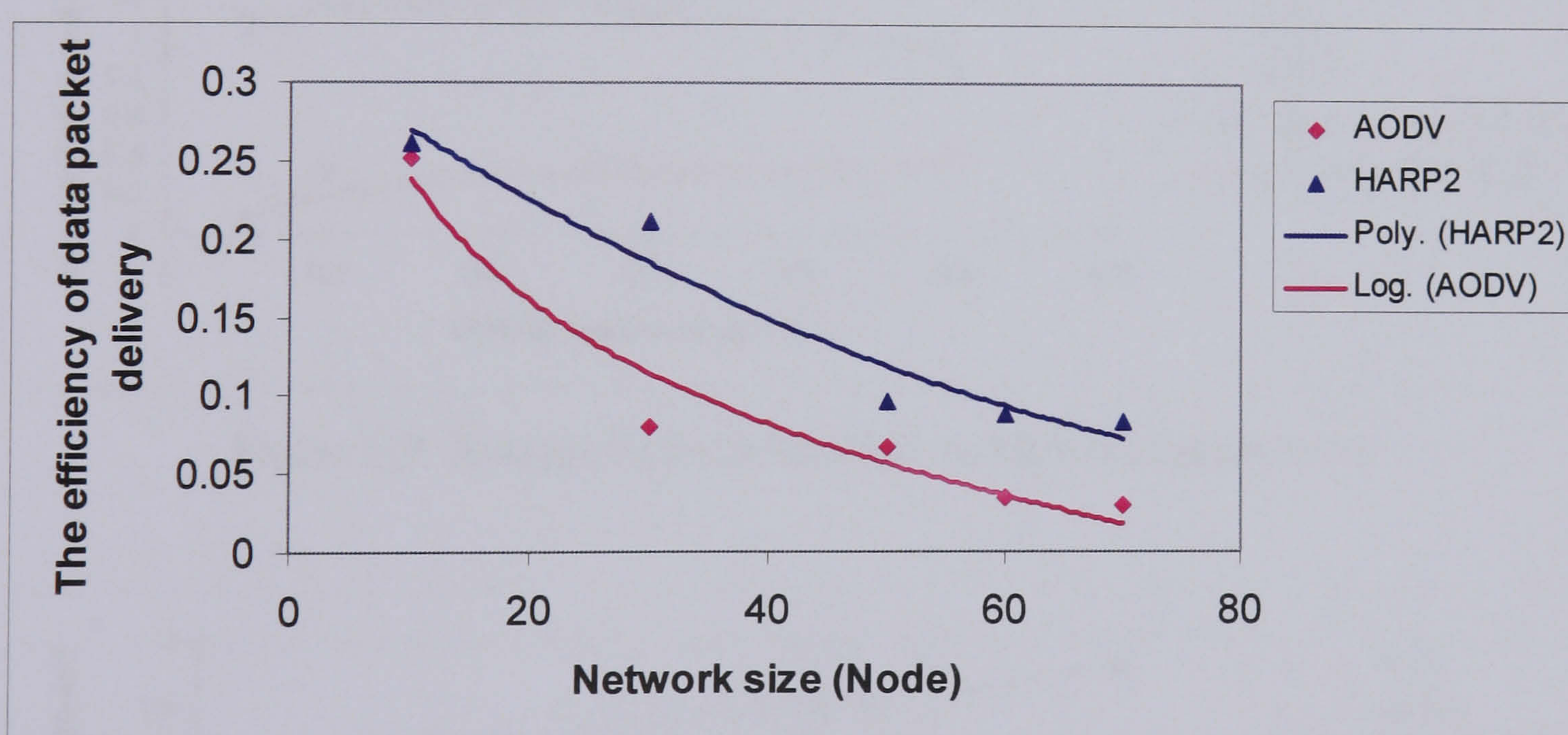


Figure 5-8: The efficiency of data packet delivery vs. Network size

Figures 5-9, 5-10 and 5-11 show the average end-to-end delay of transferred data packets against mobility with different pause time, maxima of nodes speeds, and network size. In these figures, we can see that HARP2 has an increased delay compared to the fully flooding technique protocol AODV. This is due to the delay caused by requesting the route more than one time when the node has failed to find this route on the first attempt. As can be seen in Figure 5-9, in terms of pause time, the delay is approximately steady in HARP2. When the speed of nodes is increased, the average end-to-end delay is gradually increased as shown in Figure 5-10. This is because the increased probability of link breaks caused by increasing the speed of nodes. In terms of scalability of the network, when the number of nodes is increased, the average end-to-end delay is slightly increased as well, as shown in Figure 5-11. This is due to the increased number of nodes that forms the route, which leads to more frequent breaks. The result of average end-to end-delay shown in Figure 5-11 is very similar to that one of HARP1 (Figure 4-10). This is because of the similarity in the route discovery at intermediate nodes (between the source and the destination) where each node will select one downstream node to forward the route request packets and hence the same delay is occurred.

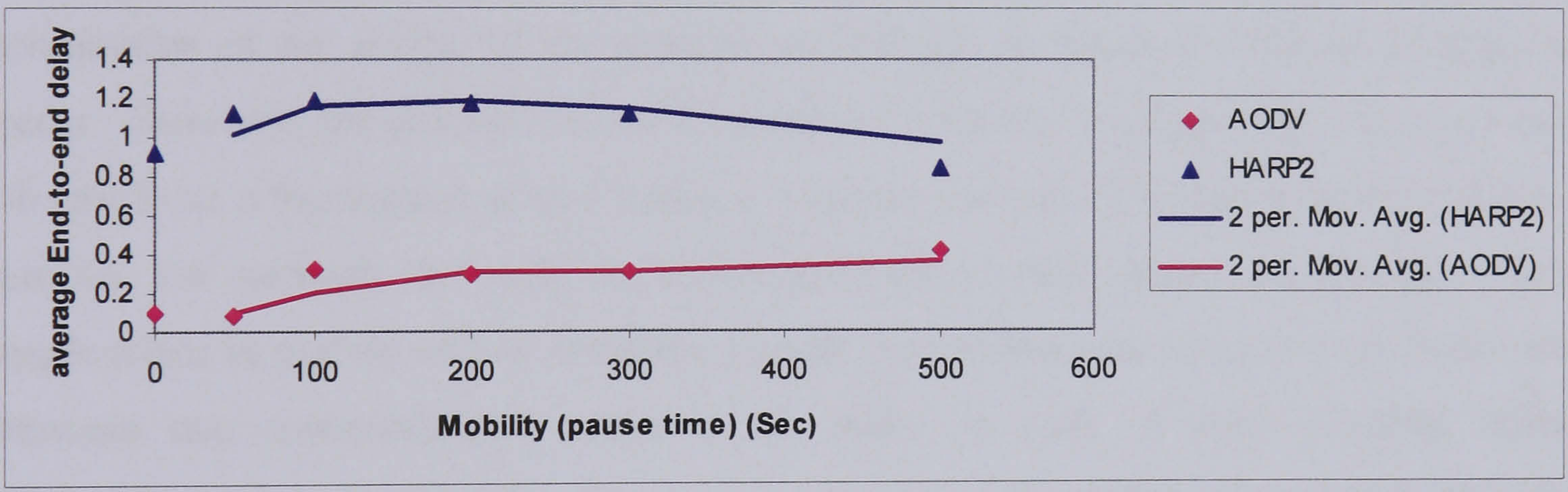


Figure 5-9: Average End-to-end delay vs. Mobility (pause time)

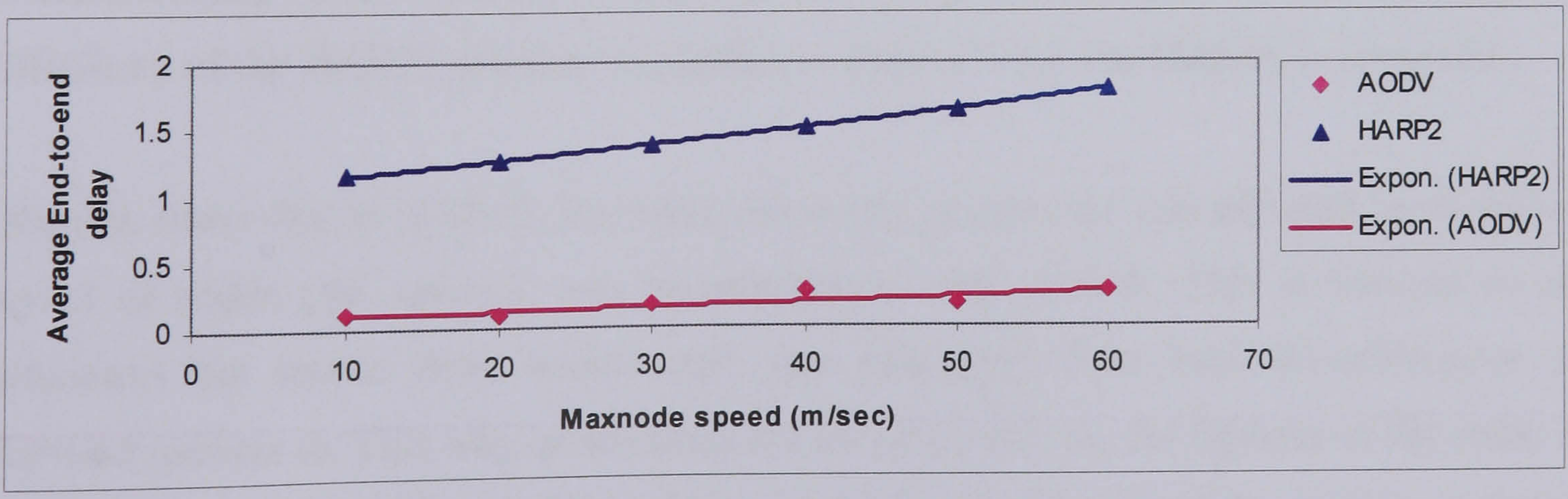


Figure 5-10: Average End-to-end delay vs. speed

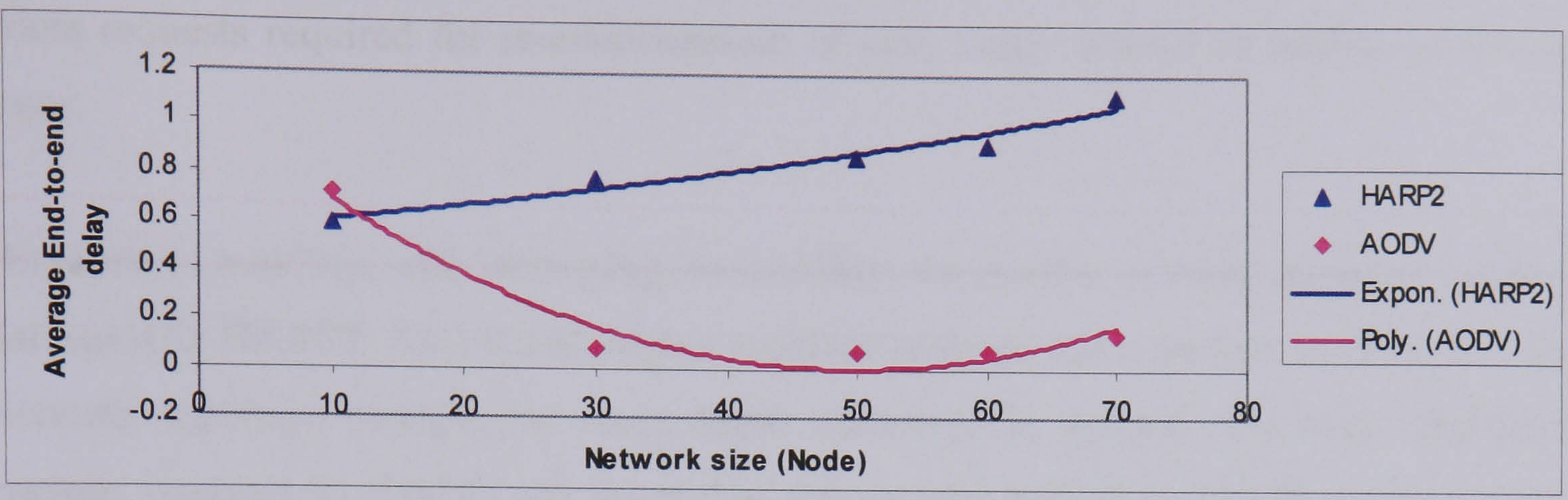


Figure 5-11: Average End-to-end delay vs. Network size

5.4 Summary

In mobile ad hoc networks, there are certain situations where the network is short of some resources of routing information used by the network (e.g., short of geographical information of mobile nodes in the network). In these situations, temporary or permanent termination of the ability of the network to perform its required function is likely to occur. Therefore, the alternative, "self-dependent" resource of information (does not rely on any fixed infrastructure or any external resources such as GPS) has to be available for use by the network in order to accomplish the needed tasks. In addition, some applications in mobile ad hoc networks require the maintenance of most long-lived path between two communication nodes in the route, in spite of some accepted delay. Moreover, some applications also require reducing the effect of mobility and the overhead of control messages used for establishment of a route between two communicating nodes. In order to meet the above requirements as well as increasing the efficiency of the HARP1 protocol explained in chapter Four, the HARP2 is proposed.

Results show that in HARP2, the route discovery packets are less affected by mobility, speed of nodes and network size in comparison with AODV. This is because in all situations the source node selects only one neighbour from each direction-zone to forward packets to. This way of selection covers all directions, the lifetime of the route is longer when selecting the neighbour that moves in near direction to the node performing the selection. In HARP2, the local repair of broken links helps in reducing the number of route requests required for re-establishment of new routes instead of broken or missed ones.

In terms of mobility, with increasing the mobility, the number of route discovery packets increases in HARP2. As a result, higher mobility requires more packets to cope with the network topology change and route break recovery. In general, the route discovery packets required by HARP2 are fewer than the packets needed in AODV protocol along all the speed range (from 10 to 60). This is due to good control and distribution of route request packets. HARP2 scales well with the network size in terms of overhead cost.

Regarding to ERDP, HARP2 has better ERDP than the ERDP of AODV with different values of pause time, speeds and different number of nodes. This means that less control packets are needed to deliver data packets from a source to a destination, because of long-lived route established by using *HDA*. In general, results show that HARP2 has an increased delay compared to the fully flooding technique protocol AODV. This is due to the delay caused by requesting the route more than one time when it is failed to find this route from the first try.

Chapter 6

HARP3 (Heading-Direction-Based Routing Protocol)

6.1 Motivation

In HARP2, the maximum number of packets propagated by the source node to its neighbours is equal to the maximum number of direction zones. In addition, the source node selects only one neighbour from each zone. Therefore, reducing the number of selected neighbouring nodes at the source node, without reducing the performance of the protocol, requires additional routing information, such as the geographical locations of nodes. This routing information requires an additional external resource of information to be available to the mobile ad hoc network. Hence, *HARP3* is assisted by geographical location information that could be provided by the Global Positioning System (GPS) [21, 22, 53]. Combining the heading direction technique with the geographical location enhances the performance of existing location-based approaches that rely only on the geographical information. In addition, it maintains long-lived routes between sources and destinations, and reduces the effect of mobility. The idea is to use the location information beside the heading direction. This is for reducing the propagation of control messages (route requests and route replies), and to control packet flooding and forwarding decisions. Another objective of the HARP3 algorithm is to investigate the usage of external resource of routing information beside the "self-dependent" metric.

6.2 The Proposed Routing Protocol

HARP3 is an on-demand routing protocol that relies on the geographical information provided to the ad hoc networks, as well as the heading direction of nodes. In HARP3, it is assumed that:

- Each node knows its own heading direction angle and location information.
- Each node propagates its heading direction angle and location information to the node's immediate one-hop neighbours in a periodic manner.
- The source node knows the position information of the desired destination node

that the source node need to send data packets to. Typically, a location service is responsible for this task.

In order to learn the current position of a specific node, the help of a location service is needed. Generally, in location service protocols, mobile nodes register their current position with a known service (or a server). When a node does not know the position of a desired destination node available in the network, it contacts the location service and requests that information. Chapter 8 describes in detail the location service approaches and the new proposed adaptive location service.

The neighbours' HDA at each node are grouped in eight zones according to the HDA and regardless to their locations. The source node *S* knows the location of the source node *D* (X_d, Y_d) at the time of which route discovery is triggered by *S*. The coordinates (X_d, Y_d) are included in the route request. In HARP3, as in other on-demand routing algorithms, the principle of constructing a route between a source node and a destination node relies on route discovery and route maintenance techniques.

6.2.1 Route Discovery

The source node initiates the route discovery by activating and preparing the route request packet to be sent toward the destination node. The route request is propagated through selected intermediate nodes, when the intended destination is not a neighbour to the source node. Through discovering the route between the source node and destination node, the route request packet and route reply packet both contribute to finding the route.

6.2.1.1 Route Discovery at the Source Node

At the source node *S*, when *S* has data packets to send to a destination *D*, *S* will need to request a route to the destination *D*. Firstly, *S* will look in its cache memory for *D*, and:

- If *D* is available in the cache, *S* will forward the data packets to *D* directly and there is no need to establishing a route to that destination.
- If *D* is not available in *S* cache memory, *S* will start preparing the route request

packet as follows:

- S sets up a time T_d, where T_d is the time required to find the destination.
- Then, *S* starts looking into its cache for a neighbour that satisfies the following two conditions:
  I) The position of the selected neighbour is the closest to the destination position among all neighbours.
  II) The selected neighbour has a nearest heading direction angle (HDA) to *S*.
    - If the neighbour is found in the cache memory, a list of route records (LRR) is then initiated as described in HARP1. A new record is added to LRR containing information about the source node (A node IP address, a node heading angle, and a zone-direction number). Then *S* will propagate the route request packet that includes the LRR to that addressed neighbour.
    - If no neighbour has satisfied the two conditions together, then *S* will select the neighbour that satisfies the first condition with the most nearest HDA to *S*.

Figure 6-1 shows the pseudo-code algorithm for HARP3 that is executed at the source node.

6.2.1.2 Route Discovery at the Intermediate/Relay Node

All intermediate nodes that receive the route request packet, will update their route cache entries by updating the information of the node, from which the packet was received. Only the intermediate node that the route request packet is addressed to and has a record in the list of route records, will accept the message; other nodes will silently drop it. The intermediate node that the packet is addressed to, will search in its cache memory of neighbours for the destination *D*, and:

- If *D* is available in the cache memory, the intermediate node will update the LRR

```
// if the number of RREQ initiated less that the maximum allowed number of RREQ
If RREQ_Count <= Max_RREQ_Count then
{
    If the node is S then
    {
      If IPAddr_D ∈ NbCache_S then          // if D is neighbour to S
      {
        Send (data packets to IPAddr_D);
      }
      Else
      {
         Init (T_d);                        // initiate T_d
         S_Dir = HDA of S;
         S_Zone = Zone number of S;
         S_Dist = Distance between S and D;
         Init (LRR);                        // initiate a List of Route Records
         //Add to LRR: S' Address, HDA of S, Zone number of S
         LRR_Add (IPAddr_S, S_Dir, S_Zone);
         δ = Step ;                         // Initial value of step angle
         NbFound = 0;
         Do
             L = S_Dir - δ;
             H = S_Dir + δ;
             // Looking for a neighbour Nb and skip the selected neighbour in
             // previous RREQ.//Nb satisfies two conditions:
             // Nb_Dist < S_Dist and H >= Nb_Dir >= L
             IPAddr = Find_Nb (S_Dist, L, H);
             If IPAddr_Nb <> 0 then         // Neighbour is found
             {
                // Forward RREQ to a neighbour Nb
                Forward_RREQ (IPAddr_Nb);
                NbFound = 1;
             }
             δ = δ + Step ;
         While ((δ≤Max_acceptable_difference_in_HDA) and (not NbFound))
         If not NbFound then
         {
            Broadcast_RREQ ();              // Broadcast the RREQ to all neighbours
         }
      }
    }
}
Else STOP                                   // do not initiate RREQ
```

Figure 6-1: Pseudo code for HARP3, RREQ at Source node S addressed to D by adding a record to it; this record contains information about the node itself. The intermediate node then sends back a reply packet along the nodes that have records in LRR. The list of route records is backtracked to the initiating source node *S*.

- If *D* is not available in the cache memory as a neighbour, the intermediate node will follow the technique of finding a neighbour in the cache memory. The selected neighbour has to satisfy the two conditions mentioned earlier. The axis mapping technique will be follow for finding a suitable neighbour nearest in direction to the intermediate node direction and nearest to the destination location. Before forwarding the request packet to the next downstream node (selected neighbour), the intermediate node will add a record to the list of route records containing information about itself. If no neighbour is found for the time Td, RREQ will be triggered again (S will repeat the route request a limited number of time e.g. 5 times in order to avoid the search-to-infinity).

To prevent the occurrence or effectiveness of loops in the search, HARP3 algorithms use a node's sequence number, in addition to the checking the availability of the selected neighbour node in *LRR* before sending the packet to that neighbour. If the neighbour is found in the list, another neighbour will be selected.

6.2.1.3 Route Reply

In HARP3, as in HARP1 and HARP2, the route reply message is triggered and sent back to the originator node of the route request in two cases:

1) The addressed destination node receives the route request packet. In this case, the destination node extracts the LRR list that is carried in the route request packet and piggybacks the LRR list in the route reply packet. The destination node then sends the route reply packet along the reversed path mentioned in the LRR list.
2) The intermediate node also triggers the route reply packet. This done when an intermediate node receives the route request packet and has fresh routing information stored in its cache about the destination (a fresh and valid path to

the destination). The intermediate node updates the LRR list by adding its information and piggybacks the LRR list in the replied message. This node then sends the message along the reversed path determined by the nodes recorded in the LRR list.

6.2.2 Route Maintenance and Local Repair

As in all reactive routing approaches, detecting the broken link in HARP3 protocol is the responsibility of each node along the established route between the source and the destination nodes. When two communicated nodes move out of each other transmission range, the connection between them will be disconnected. The link breakage can be detected if a node receives a link layer feedback signal from the wireless MAC protocol such as IEEE 802.11 [44]. The link is considered unavailable in the following main cases:

1. The period T_d is expired at the intermediate node during route request.
2. T_n is expired (T_n is a time set by a node to find its neighbours) and the intermediate node cannot hear or finds any neighbour.
3. A downstream node cannot find the upstream neighbour that has a record in *LRR*.

An error message is prepared. This message is then sent back to previous node **(Local Repair)** to perform axis mapping, and to find new neighbour to propagate the message.

6.3 Simulation Methodology and Model

Studying and investigating the behaviour of the networks in different environments and different parameters by simulation is the commonly used method in mobile ad hoc networks. Consequently, simulation is the most common tool used by researchers for developing, evaluating, and comparing ad hoc routing protocols. As mentioned previously in chapter Four (subsection 4.3), many researchers in MANET have evaluated and simulated their works using different approaches and simulation tools. The most popular network simulators are: the Network Simulator NS-2 [99][100], Global Mobile Information System Simulation Library GloMoSim [101], and OPNET Modeler [102], some works has been simulated by using one of the Programming Languages as C, C++, and Java [75][103].

6.3.1 Simulation Environment

The performance of the routing protocol HARP3 has been evaluated by simulation. NS-2 was used to perform extensive simulations and to evaluate HARP3 protocol and to compare it with the conventional routing protocol AODV.

6.3.2 Parameter Values

In order to evaluate HARP3, without lose of generality, the network space for each simulation was chosen as 1000 metre x 1000 metre. The simulation time is lasting for 500 seconds.

In terms of communication model, the network traffic was modelled as 10 Constant Bit Rate (CBR) sources. The IEEE 802.11 Medium Access Control (MAC) Distributed Coordination Function (DCF) [44] protocol is used in the simulation to get the link breakage feedback signal. Radio propagation range for each node was 250 meters and channel capacity was 2 Mbps. The propagation model used in the simulation combines both a free space propagation model and a two-ray ground reflection model. A data payload generated by the source node was chosen to be 512 bytes in all the simulation scenarios.

A Random WayPoint (RWP) [106] mobility model is used for different values of pause time, max node speed, and network size. The random waypoint model is one of the most widely used mobility models in performance analysis of mobile wireless networks. For more details about the RWP, researcher refers to chapter Five.

HARP3 is evaluated with different number of nodes distributed randomly within the simulation area. HARP3 is also simulated with different values of speeds and mobility (pause time). Table 6-1 provides a summary of the rest of the simulation parameters. The results presented are mean values of multiple runs for each scenario and collected data were averaged over those runs. For fair comparisons, the same environment, set of mobility, and traffic scenarios are used in all simulated HARP3 routing scheme and AODV protocol.

Table 6-1: Parameters values
Used with NS-2 to evaluate HARP3

Scenario Name	*Pause Time Scenario*	*Max Node Speed Scenario*	*Network Size Scenario*
Pause time (s)	0,50,100,200, 300,500	10	10
Max Node Speed (m/s)	10	10,20,30,40,50,60	10
Number of mobile nodes	50	50	10,30,50,60,70
Simulation Time (s)	500	500	500
Network Space	1kmX1km	1kmX1km	1kmX1km
Radio range	250m	250m	250m
MAC Protocol	IEEE 802.11	IEEE 802.11	IEEE 802.11
Radio propagation model	Free space/ two-ray	Free space/ two-ray	Free space/ two-ray
antenna model	Omni Antenna	Omni Antenna	Omni Antenna
Traffic pattern	CBR	CBR	CBR
Maximum number of connections	10	10	10

6.4 Simulation Results and Analysis

This section consists of two main parts, the performance metrics used for evaluating the performance of the HARP3 routing protocol, and the results extracted from the simulation with the analysis of these results.

6.4.1 Performance Metrics

The same as in HARP1 and HARP2, in order to evaluate HARP3, the following performance metrics are used for evaluation:

- ***The Route discovery packets (the Overhead)*** are defined as the number of all control packets generated by all nodes in the network in order to establish routes between sources and destinations.

- ***The efficiency of data packet delivery*** is defined as the measured ratio of the number of data packets delivered to the destinations to the number of all packets generated in the networks. Note that each time a packet is forwarded is counted as one packet transmission. This metric is used to investigate how efficiently control packets and the selection of long-lived routes are utilised in delivering data packets.

- ***The Average end-to-end delay*** of transferred data packets includes all possible delays caused by buffering during route discovery, queuing at the interface-queue, retransmission delays at the medium access control layer, propagation and transfer times, and ARP delay.

Each parameter metric mentioned above was simulated in three different scenarios:

7) Mobility scenario: with different pause time values,
8) Speed scenario: with different node speeds,
9) Network size scenario: with different number of nodes.

6.4.2 Results and Analysis

The solid lines in Figures 6-2, 6-3, 6-4 and 6-5 show an appropriate line of best fit to the experimental data. Figure 6-2 depicts the route discovery packets against mobility with different pause time. From Figure 6-2 it can be seen that with increasing the mobility of nodes in the network, the number of control packets required for discovering the route in HARP3 is increased. This is due to the fact that, higher mobility of nodes in the network requires more packets to cope with the network topology change and route breaks recovery. In addition, it can be seen that the number of route discovery packets needed to find the path is much less in HARP3 compared to AODV protocol. This is because of that HARP3 has adopted the selective technique that selects some few nodes to be used in forwarding the packets. Another reason is the flooding technique used in AODV that causes higher overhead control packet than the technique used in HARP3.

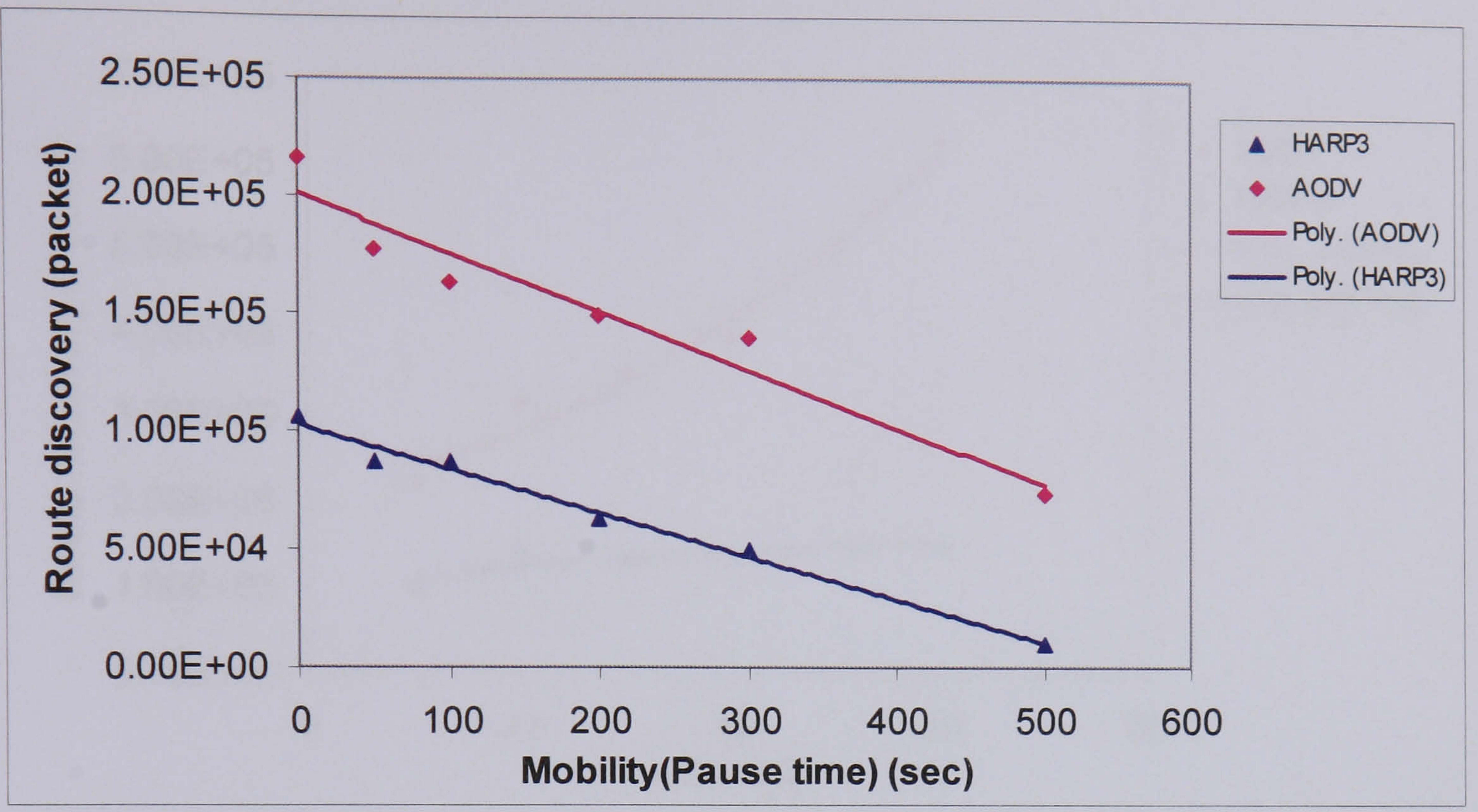


Figure 6-2: Route Discovery vs. Mobility (Pause Time)

The impact of nodes speeds on the route discovery packets is shown in Figure 6-3. It can be seen that when the speeds of nodes are less than 20 m/s (low speeds), the route discovery packets needed to find the path in HARP3 are increasing gradually but at speed of 20 m/s and higher, the route discovery packets become nearly steady across all the speed range (from 20 to 60). In general, as can be seen in Figure 6-3 the route discovery packets required by HARP3 are much fewer than the packets needed in AODV protocol along all the speed range (from 10 to 60). This is due to that during establishing the routes, and in all situations, the source nodes and intermediate nodes select some nodes to contribute in finding these routes. This leads to a good distribution of route request packets. In addition, as speed increases, the number of route discovery packets generated by AODV increases rapidly due to the storm of flooding.

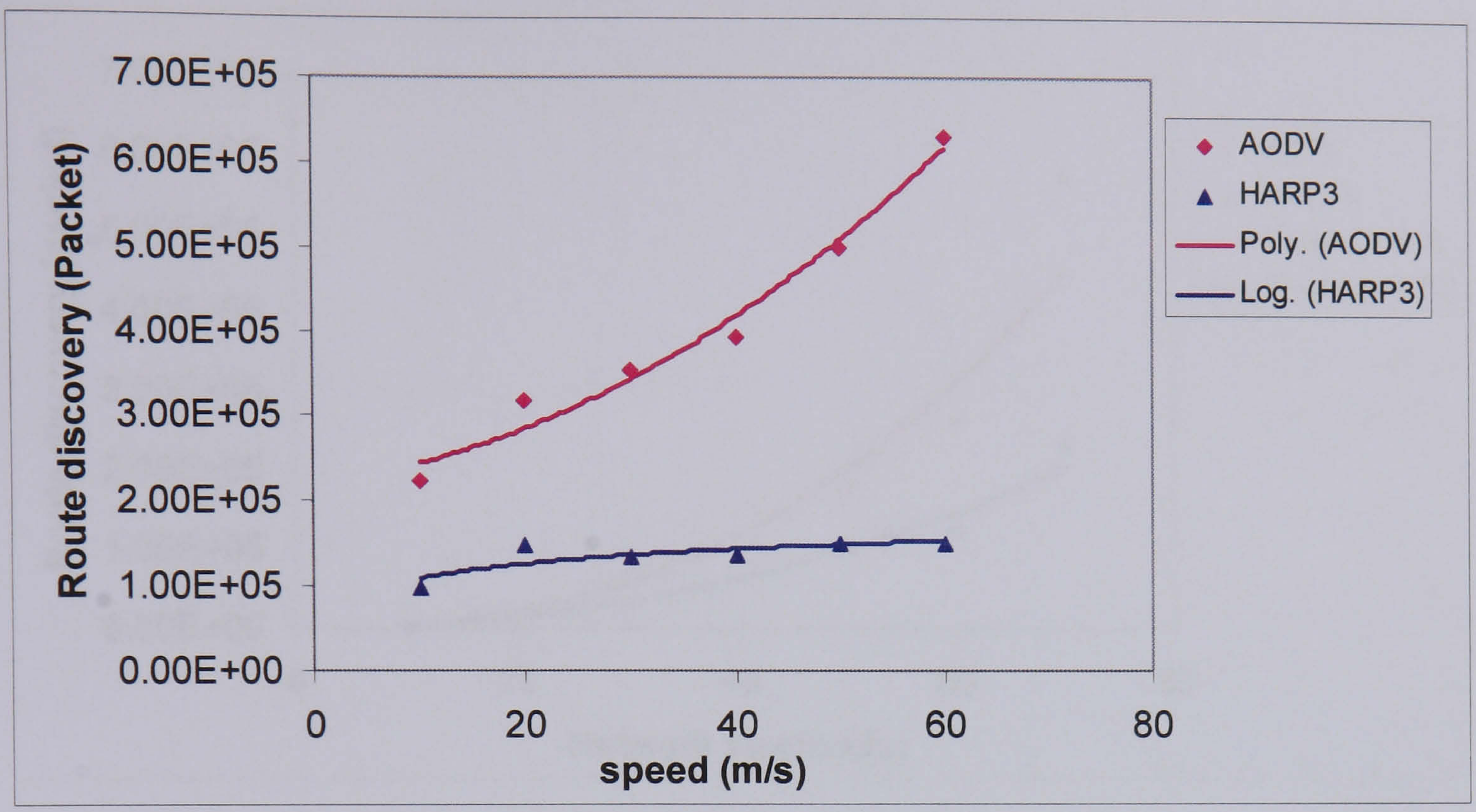


Figure 6-3: Route Discovery vs. speed

The scalability of mobile ad hoc networks with the number of nodes is shown in Figure 6-4. As can be seen in Figure 6-4 as the number of nodes in the network increases, the number of route discovery packets generated by HARP3 gradually increases, compared with the AODV. When the number of nodes is greater than 60 (Node# > 60), the number of route discovery packets required to find the path in HARP3 is increasing slowly in comparison with AODV where this slope increases sharply. This leads to the conclusion that HARP3 is more scalable with the network size in terms of overhead cost than the AODV.

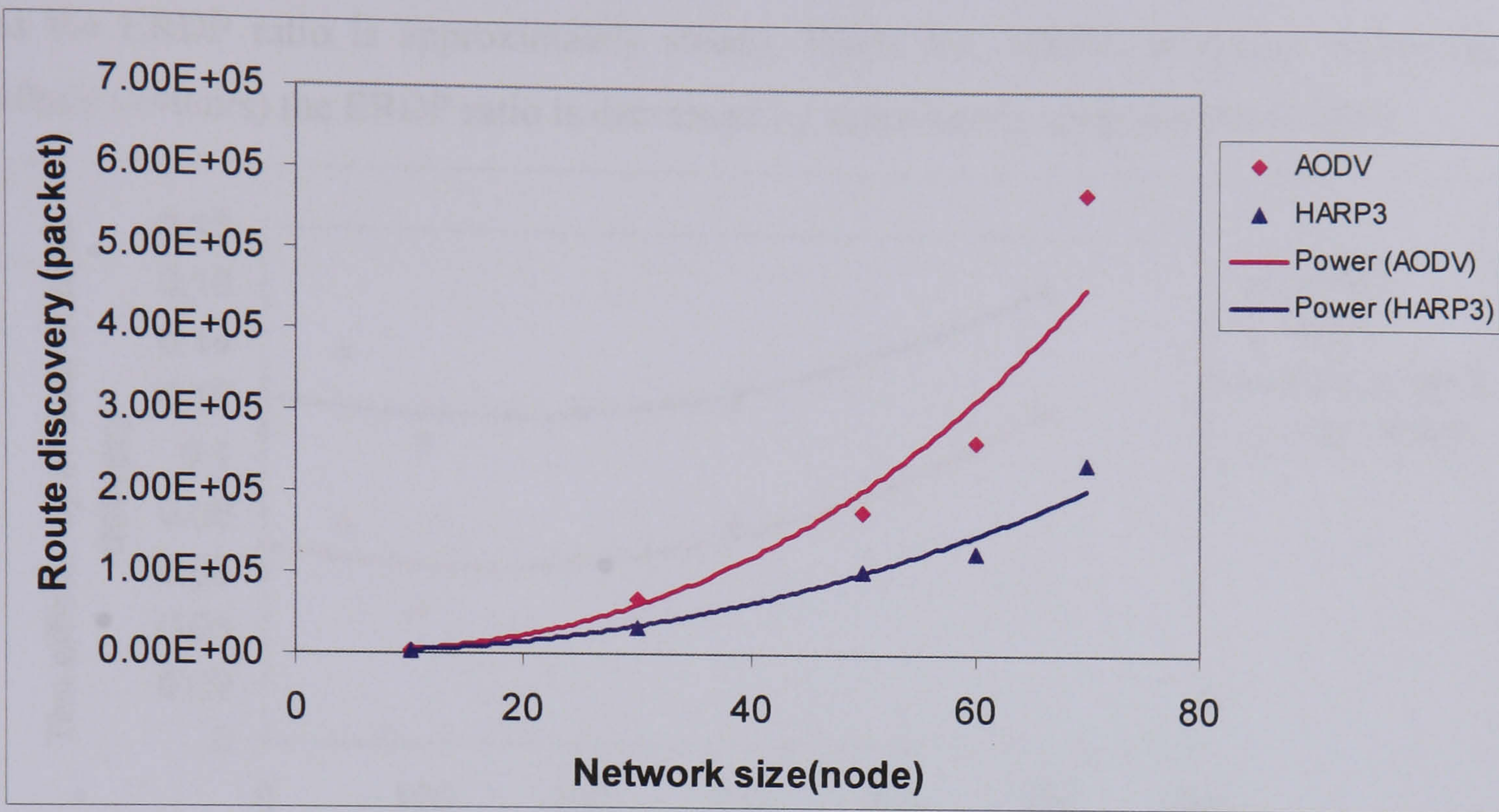


Figure 6-4: Route Discovery vs. Network size

The route discovery packets in HARP3 are less affected by mobility, node speed and network size than AODV.

Figures 6-5, 6-6 and 6-7 show the efficiency of HARP3 represented by ERDP against mobility with different pause time, maxima of node speeds, and network size. Higher ERDP ratio means better performance and good efficiency. In general, as can be seen in these figures, ERDP in the HARP3 is higher than the ERDP of AODV in terms of different values of pause time, speeds and different number of nodes. This means that fewer control packets are needed to deliver data packets from source to destination nodes, due to the long-lived route established by using HDA.

In Figure 6-5, when the mobility of nodes increases, the ERDP ratio increases gradually in both simulated protocols. This is because of the increasing number of packets generated in the network in order to establish the required routes.

Figure 6-6 depicts the ERDP ratio against the speed of mobile nodes. It can be seen from this figure that at low speeds (10-20m/s) in both simulated protocols (AODV and HARP3), the ERDP decreases. At higher speed (>20m/s), HARP3 shows good efficiency as the ERDP ratio is approximately steady. While for AODV, at speeds higher than 40m/s (>40m/s) the ERDP ratio is decreased by significantly compared to HARP3.

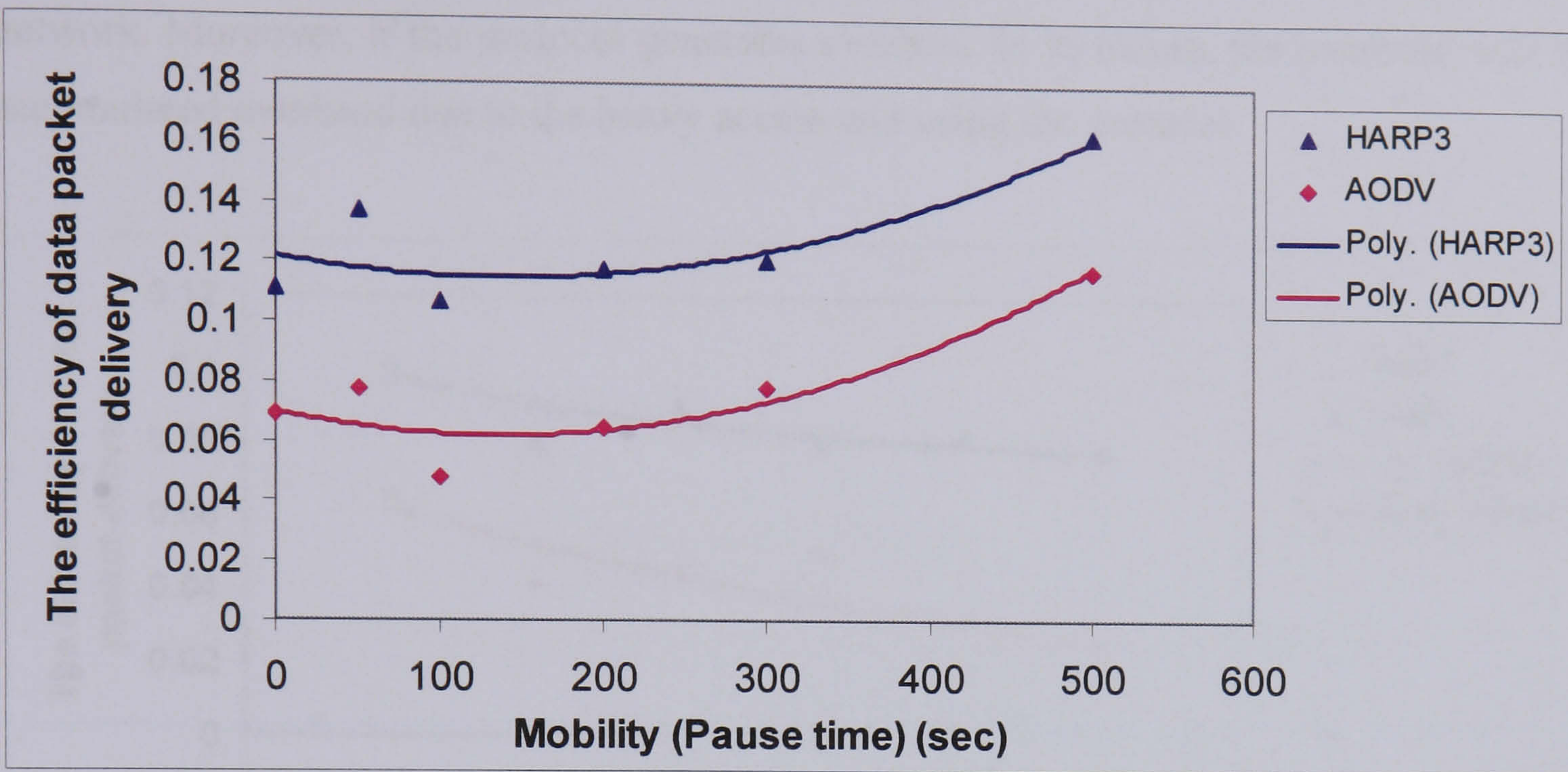


Figure 6-5: The efficiency of data packet delivery vs. Mobility (pause time)

Regarding to the scalability of the network with the number of mobile nodes, Figure 6-7 represents the ERDP ratio against number of nodes. When the number of mobile nodes increases to 50 nodes, the ERDP ratio for HARP3 decreases sharply. For greater than 50 nodes (nodes# >50), the ERDP becomes nearly steady. This leads to a conclusion after a limited number of nodes; HARP3 is not affected by further increasing the number of nodes. The ERDP ratio for AODV, however, continues decreasing as the number of nodes is increasing. Consequently, when the number of nodes in ad hoc network is high, higher number of nodes will contribute in the formation of the route, which leads to higher probability of link breaks and thus, more control packets needed to repair or re-establish broken routes.

In relation to average end-to-end delay metric, by utilising and adopting flooding technique, it is most likely to find the required path in short time with an acceptable delay at the expense of significant overhead, more collisions, and no guarantee to select the path that lasts for acceptable period. In most of the applications, it is crucial and important to find the path that lasts longest with reduced overhead and collision and with an acceptable level of delay. This is necessary especially in applications that require heavy access to the network by users. The heavy access will cause more overhead in the network. Moreover, if the protocol generates overhead in its nature, the overhead will be accumulated overhead due to the heavy access and using the protocol.

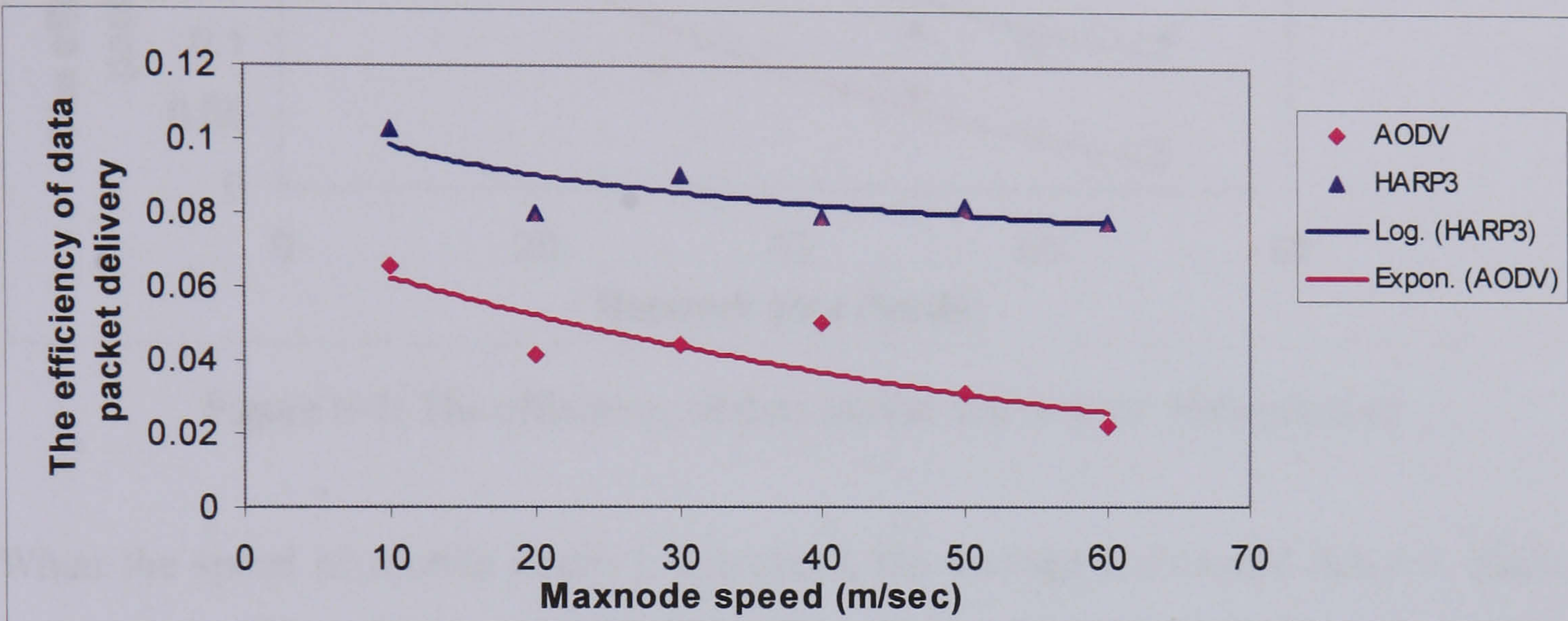


Figure 6-6: The efficiency of data packet delivery vs. speed

The average end-to-end delay of transferred data packets against mobility with different pause time, nodes speeds and network size (number of mobile nodes in the network) are depicted in the Figures 6-8, 6-9 and 6-10. In these figures, it can be seen that HARP3 has an increased delay compared to the fully flooding technique protocol AODV. This is because HARP3 reduces the blind flooding by only forwarding the route request packets to a node that is close to the destination and with near heading direction to the node in process. As a result, a higher delay will occur when establishing the path to the destination.

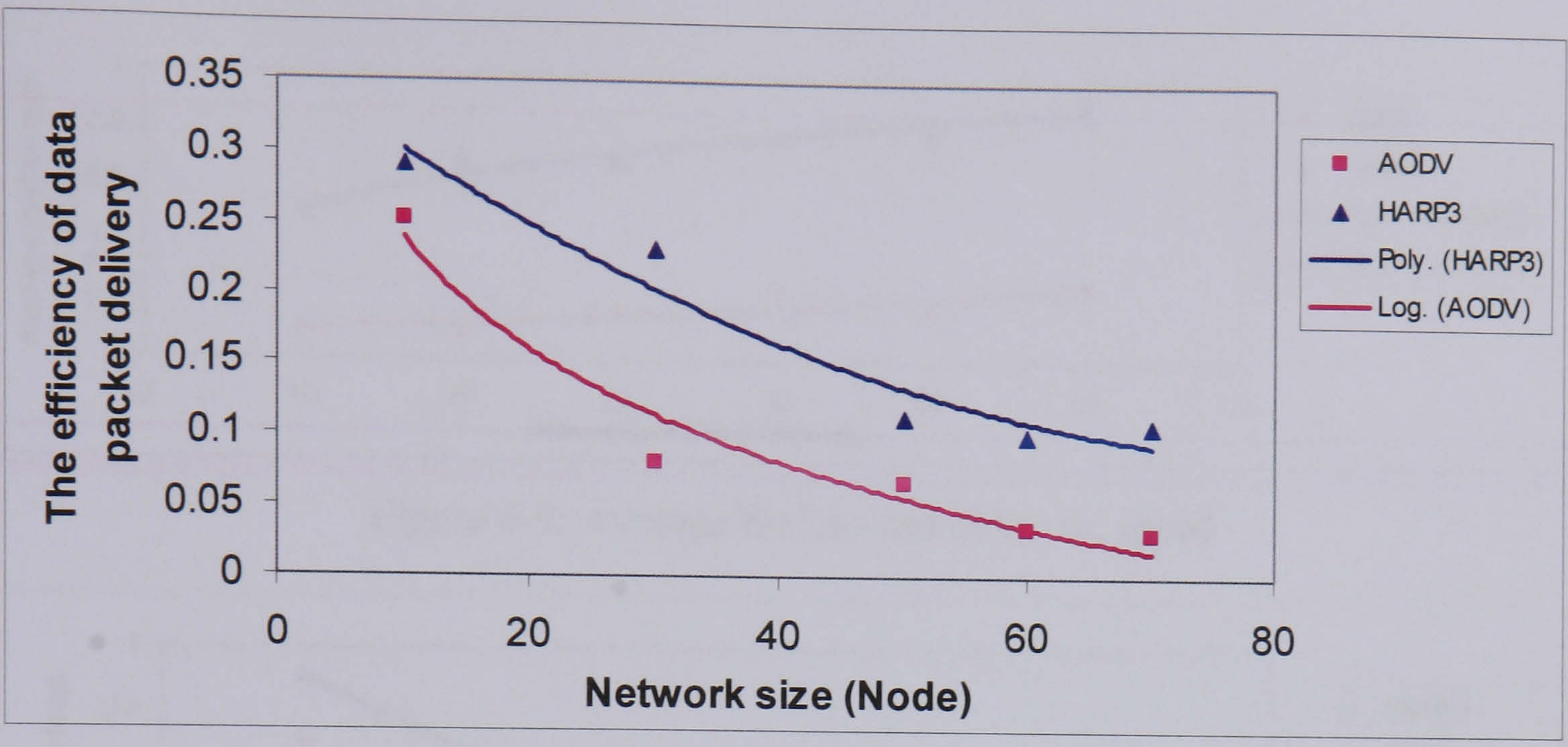


Figure 6-7: The efficiency of data packet delivery vs. Network size

When the speed of mobile nodes is increased, the average end-to-end delay is slightly increased as shown in Figure 6-9. This is because the higher probability of link breaks caused by increasing the speed of nodes. In terms of scalability of network, when the number of nodes increased, the average end-to-end delay is decreased as well as shown in Figure 6-10. This is due to the greater availability of neighbouring nodes to select from as a next hop toward the destination. In AODV, the end-to-end delay is nearly steady when number of nodes is higher than 30 because the transmission storm caused by contributing all nodes in the network in flooding the route request packets, which in turn reduce the delay of finding the route to the destination. However, this is on the cost of heavy overhead of control packets, which consume the bandwidth used by the network.

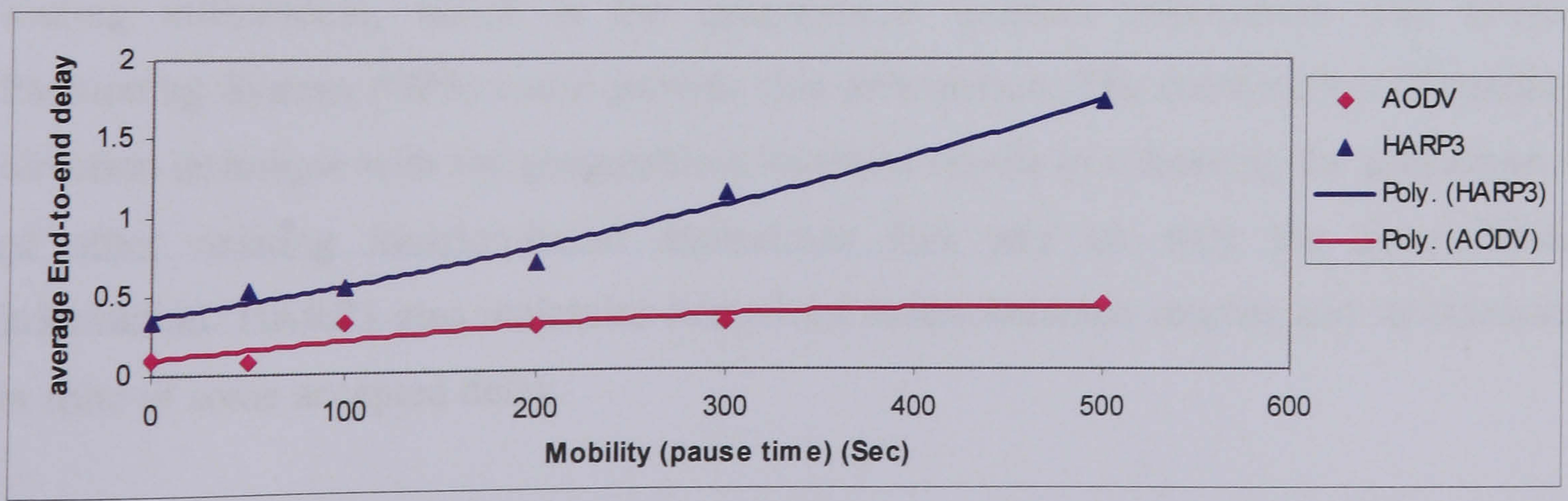


Figure 6-8: Average End-to-end delay vs. Mobility (pause time)

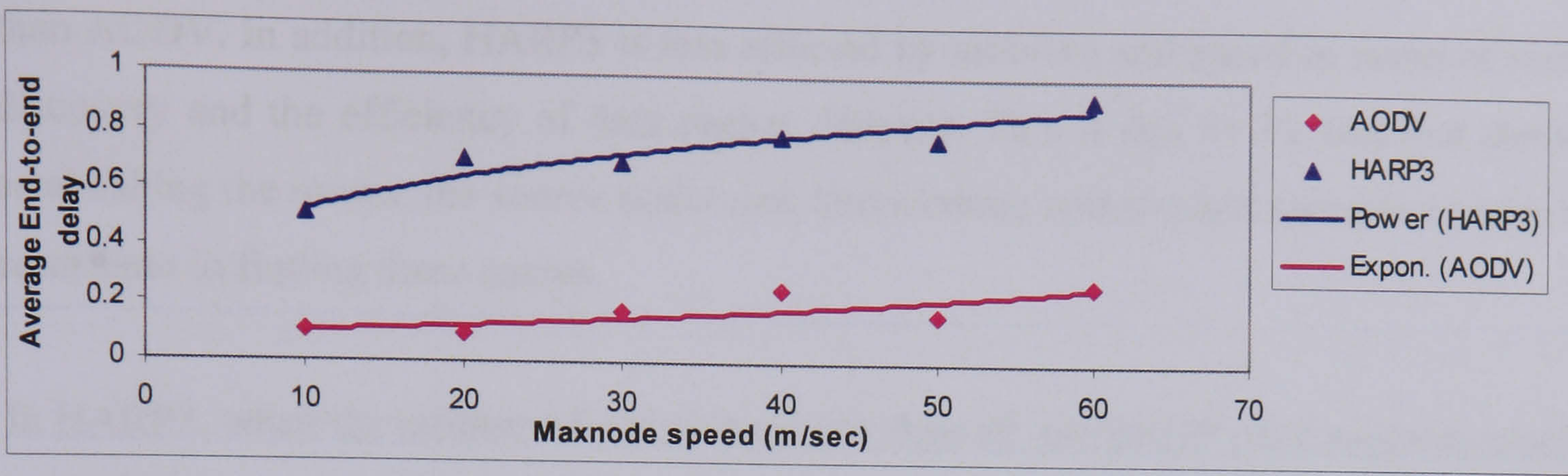


Figure 6-9: Average End-to-end delay vs. speed

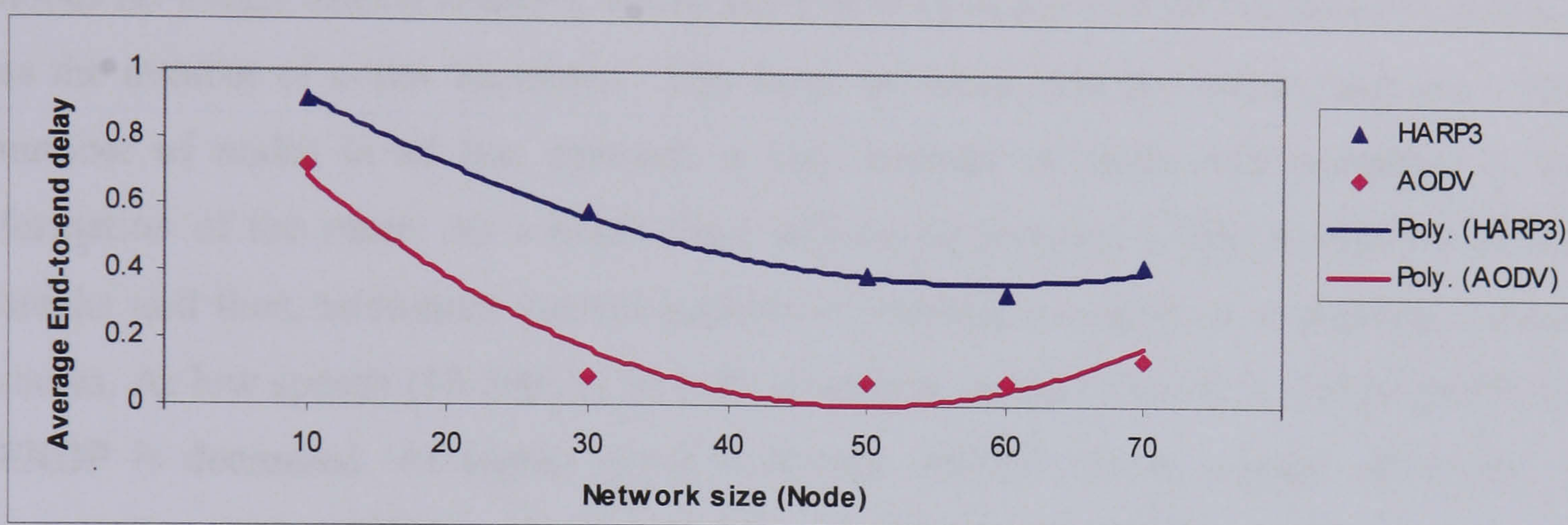


Figure 6-10: Average End-to-end delay vs. Network size

6.5 Summary

In this chapter, the third proposed routing protocol named HARP3 has been introduced. This protocol, in addition to the heading direction information, is assisted by external routing information, which is the geographical location information. The Global Positioning System (GPS) could provide this information. The combination of heading direction technique with the geographical locations results in enhancing the performance of other existing location-based approaches that rely on only the geographical information. HARP3 also maintains long-lived routes between sources and destinations in spite of some accepted delay.

This routing protocol has been evaluated by using the Network Simulator NS-2. Results show that the HARP3 is more scalable with the network size in terms of overhead cost than AODV. In addition, HARP3 is less affected by mobility and speed in terms of route discovery and the efficiency of data packet delivery. This is due to the fact that during establishing the routes, the source nodes and intermediate nodes select some few nodes to contribute in finding these routes.

In HARP3, when the number of nodes is greater than 50, the ERDP ratio becomes nearly steady. This means that after a limited number of nodes, an increased in the number of nodes no longer affects HARP3. whilst the ERDP ratio for AODV continues to decrease as the number of nodes increases. This leads to conclusion that when there are a high number of nodes in ad hoc network, a high number of nodes will contribute in the formation of the route. As a result there will be an increase in the probability of link breaks and thus, additional control packets are needed to repair or re-establish broken routes. At low speeds (10-20m/s), in both simulated protocols (AODV and HARP3), the ERDP is decreased. At higher speed (>20m/s), HARP3 shows a good efficiency, in comparison with AODV, as the ERDP ratio is approximately steady.

One drawback of HARP3 is that it has an increased average end-to-end delay compared to the fully flooding technique protocol AODV.

In HARP3, the using of local repairs to broken links helps in reducing the number of route requests required for re-establishing new routes to correct the of broken or missed ones.

Chapter 7
Comparative Analysis of Routing Protocols

This chapter describes a study that provides a quantitative analysis comparing the performance of the three proposed algorithms of multi-hop wireless ad hoc network routing protocols. Results of detailed simulations are presented, showing the relative performance of these proposed routing algorithms for ad hoc networks HARP1, HARP2 and HARP3.

In this chapter, the particular parameters and values that were chosen when implementing each algorithm in the network simulator are described. The protocols were carefully implemented in the network simulator NS-2 according to the specifications and guidance of implementing new routing algorithm issues from the designers of the NS2. In particular, in the process of implementing each protocol, some modifications for each implemented algorithm were added that improved its performance. These improvements are:

- Each of these protocols used link breakage detection feedback from the 802.11MAC layer that indicated when a packet could not be forwarded to its next hop.
- Each implemented algorithm used a local repair technique in order to repair broken links when the broken link is closer to the destination than the source node.

7.1 Experimental Design

The essential goals of the experiments are to measure the behaviour of the proposed algorithms in different network environments, under a range of conditions and to measure their reaction to network topology changes. To achieve these goals, the basic methodology was to apply different scenarios to a simulated network.

The three proposed algorithms were compared with the conventional ad hoc on-demand distance vector routing protocol (AODV) based on simulations run using NS-2 simulator.

In order to enable direct fair comparisons between the protocols, it was critical to challenge the algorithms with identical environmental conditions. Since each algorithm was simulated in the same environment as other algorithms, the performance results of the four algorithms (HARP1, HARP2, HARP3, and AODV) can be directly compared.

The protocols are evaluated by using the route discovery packets (the overhead), the efficiency of data packet delivery, and the average end-to-end delay. The simulator NS-2 version 2.27 was run on an Intel Pentium IV-based PC under the Fedora version of Linux. The Fedora is a Red Hat sponsored and community supported open source project. Each run of the simulator takes 500 seconds of elapsed time.

7.1.1 Verification of Simulation Models

To ensure that the implementations of the algorithms into the network simulator NS-2 were faithful to the protocol's specifications, the following procedures were gone through:

- The NS-2 was studied fully. This includes the C++ part; and Object Tool Command Language (OTcl) part as a command and configuration interface.
- The entire tutorial, examples, and the documentation that describe the implementation of new algorithm in NS-2 and explain creating the link between the C++ code and the OTCL code were studied.
- The codes of other routing algorithms implemented in NS-2 were fully studied and understood, such as the AODV algorithm code that is implemented in NS-2.
- The code of NS-2 was studied and fully understood, such as studying the code for programming the mobile node and its components and specifications (Figure 7-1), since it is used in the algorithms implementation.
- Each algorithm implementation was studied and verified by at least two independent experts in the C++ language.

- The result files of the simulation were traced by tracing some packets from the sender node to the received node.

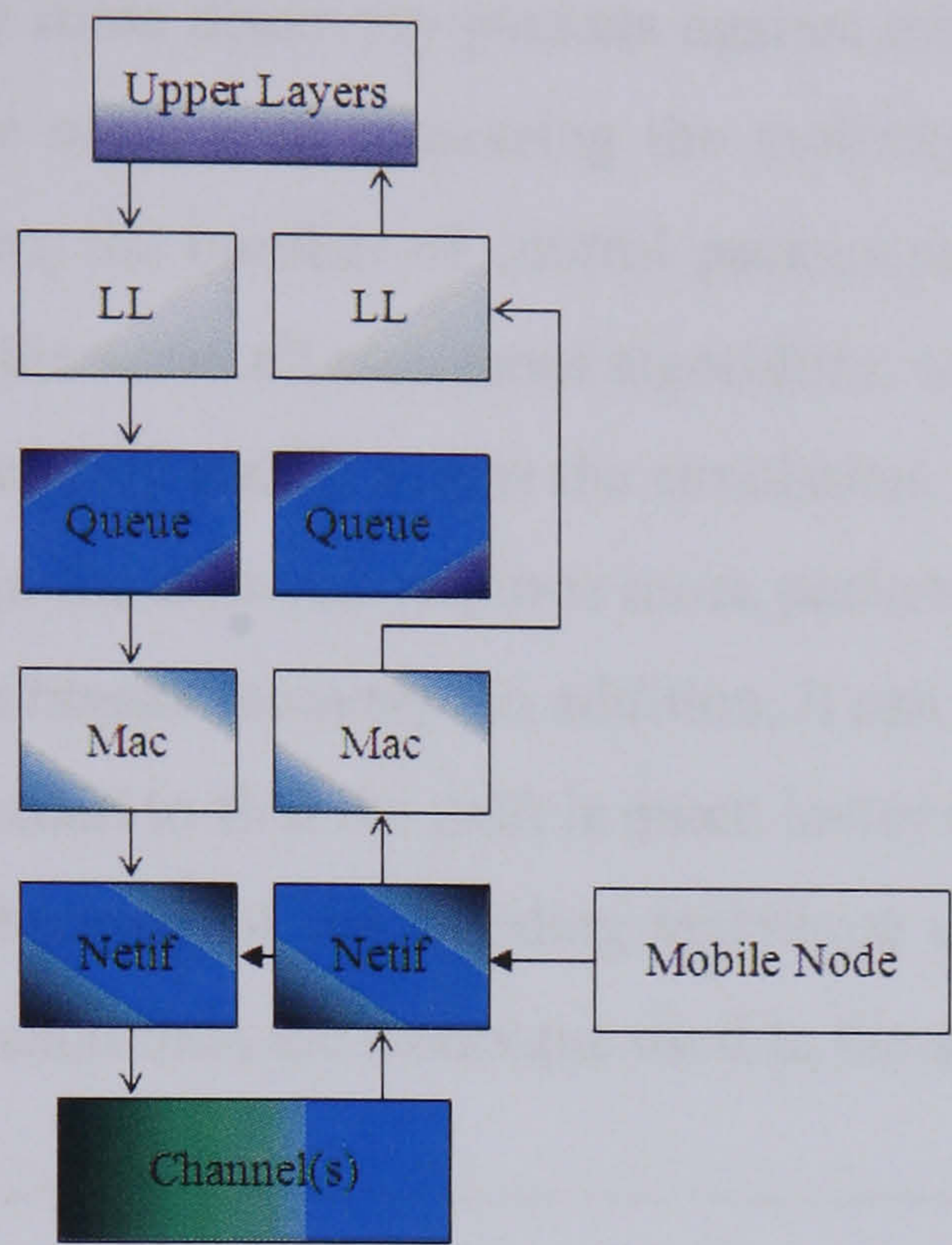


Figure 7-1: Schematic of a wireless mobile node under the NS-2

7.2 Comparison Results and Analysis

This section consists of two main parts, the performance metrics used for evaluating and comparing the performance of the routing algorithms, and the comparison overview with the analysis of these comparisons.

7.2.1 Performance Metrics

The same performance metrics used for evaluating HARP1, HARP2, HARP3 algorithms are used for the comparison.

7.2.2 Comparison Overview and Analysis

This section highlights the performance parameters used for comparing the three proposed algorithms with the AODV protocol.

7.2.2.1 The Route discovery packets (the Overhead)

The Figure 7-2 depicts the route discovery packets against mobility with different pause time (0 - 500). As can be seen, with increasing the mobility of nodes in the network (decreasing the pause time), the number of control packets required for discovering the route is increased. This is the same all compared algorithms, except in HARP1 where the route discovery is approximately steady across the simulation. This is due to the fact that, higher mobility of nodes in the network requires more packets to cope with the network topology change and route breaks recovery. In addition, it can be seen that the number of route discovery packets needed to find the path is much lower in all schemes compared to AODV protocol. This is because of the flooding technique used in AODV that causes higher overhead control packet than the technique used in the schemes.

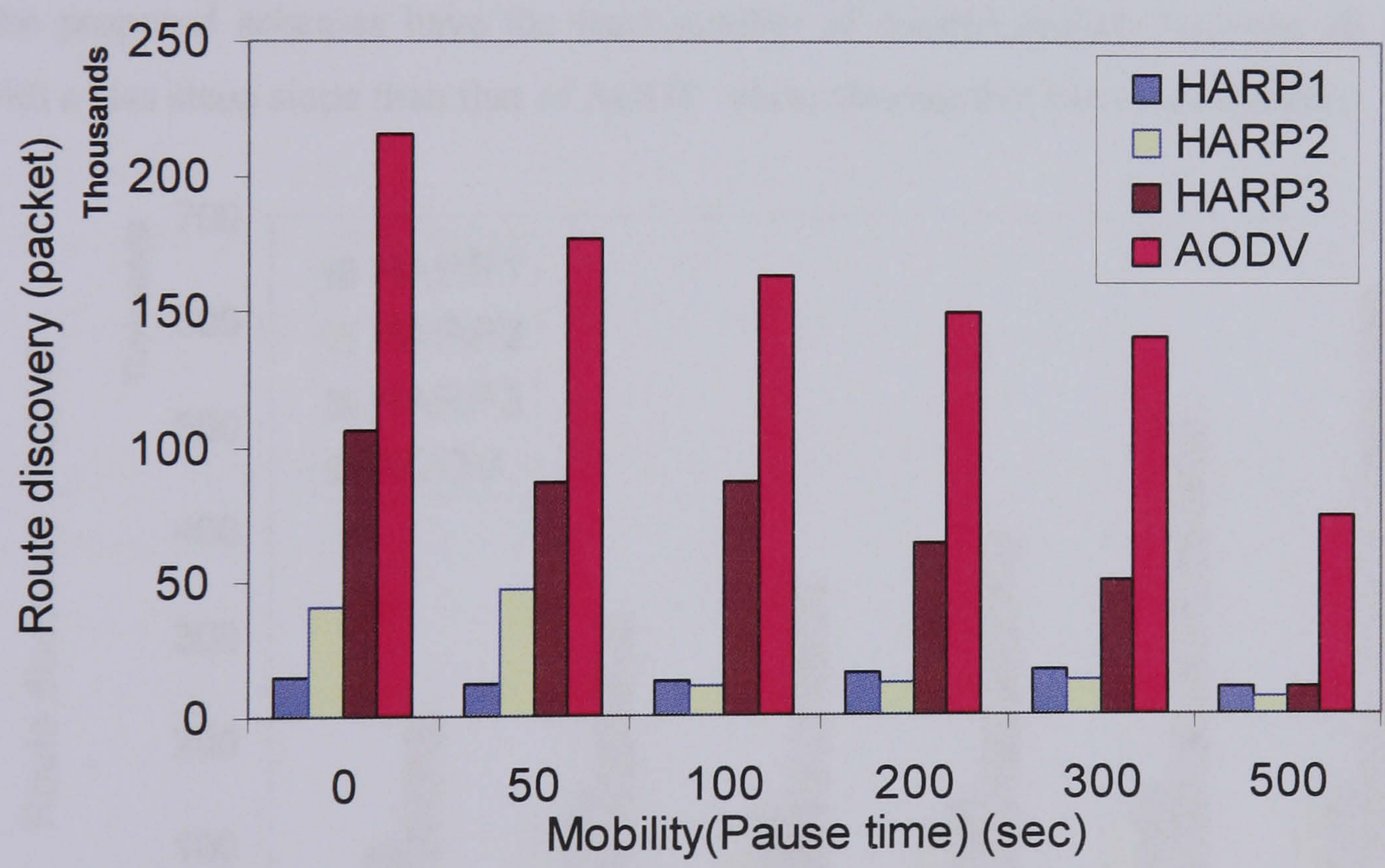


Figure 7-2: Route Discovery vs. Mobility (Pause Time)

The impact of node speeds on the route discovery packets for all schemes is shown in Figure 7-3. It is experimented the route discovery with different speeds of node movement. As speed increases, the number of route discovery packets generated by AODV increases rapidly due to the storm of flooding. Route discovery packets in all schemes significantly lower than that generated by AODV. As can be seen in Figure 7-3, in HARP2 and HARP3 at low speeds (< 20 m/s), the route discovery packets needed to find the path are increasing gradually. At speed higher than 20 m/s, the route discovery packets for all schemes become nearly steady along all different speed range. This is due to that during establishing the routes, and in all situations, the source nodes and intermediate nodes select a limited number of nodes to contribute in finding these routes. This is will lead to well distribution of route request packets.

The scalability of mobile ad hoc networks with the number of nodes is shown in Figure 7-4. In this experiment, it is experimented the route discovery packets with different number of mobile nodes. As can be seen in Figure 7-4, as the number of nodes in the network is increased, the number of route discovery packets generated by AODV is increased, and thus more control packets are needed in comparison with other schemes. The proposed schemes have the least number of control packets between all schemes with a less sleep slope than that of AODV where this number increases sharply.

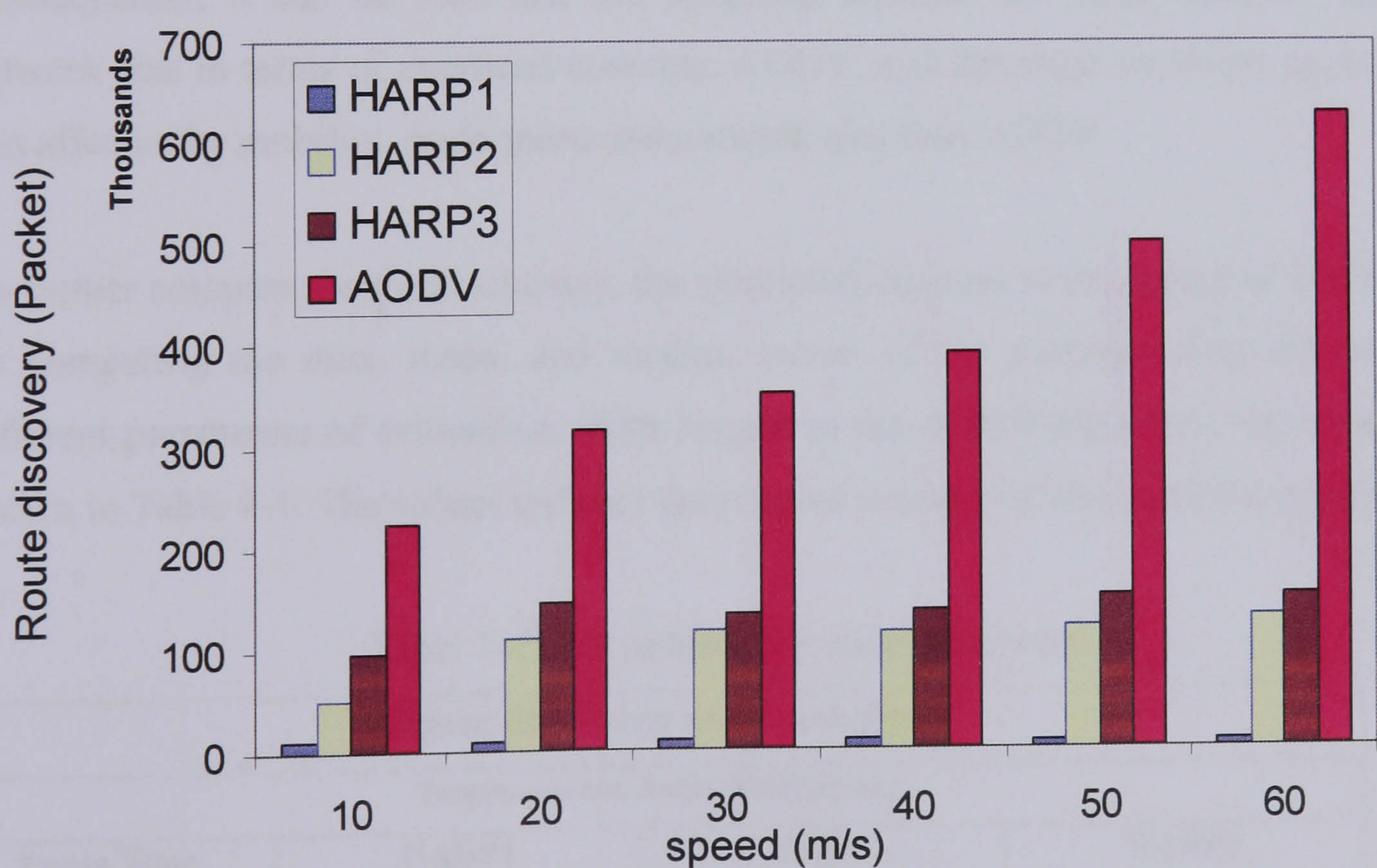


Figure 7-3: Route Discovery vs. speed

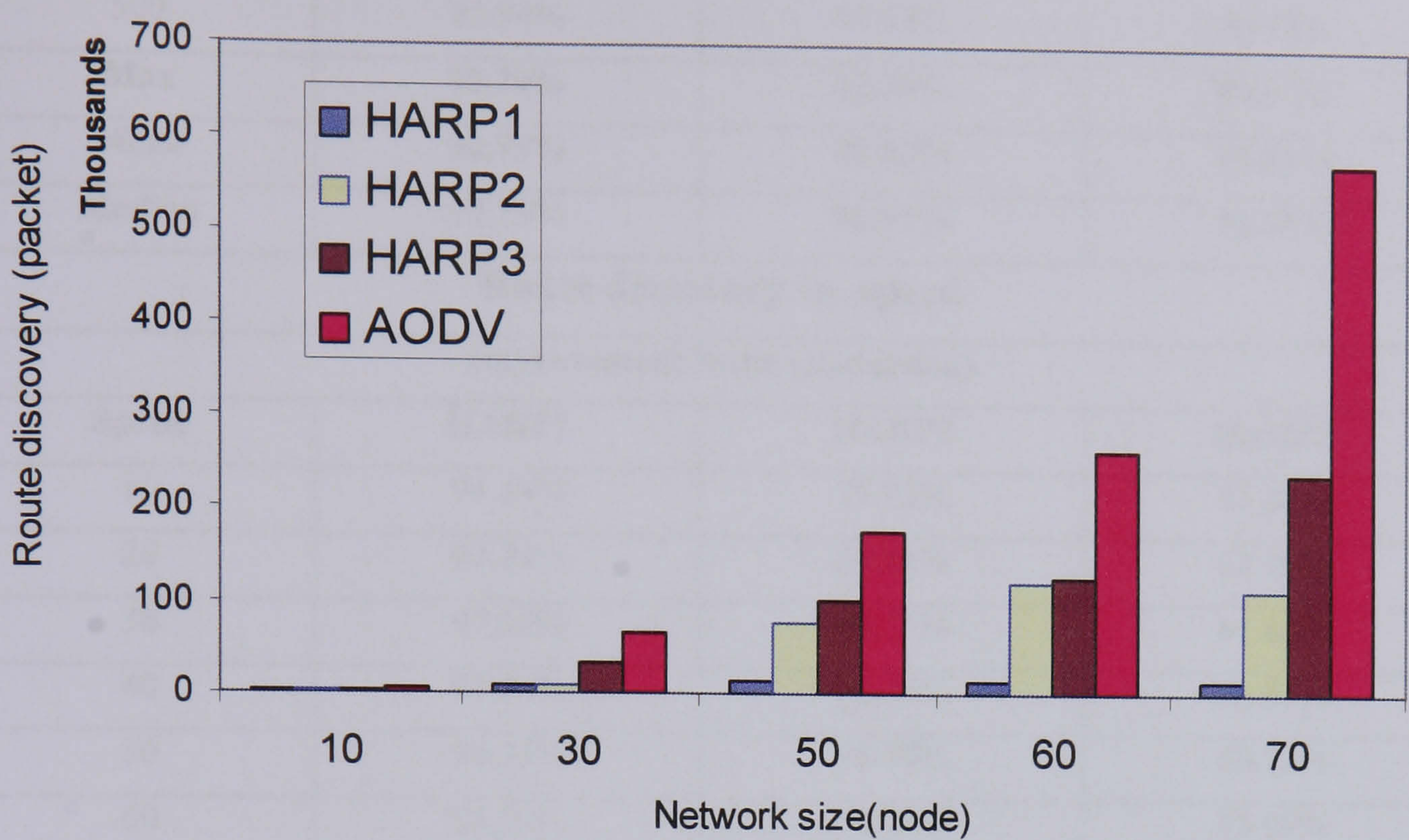


Figure 7-4: Route Discovery vs. Network size

Consequently, it can be seen that the proposed schemes are more scalable with the network size in terms of overhead cost than AODV, and the route discovery packets are less affected by mobility, node speed and network size than AODV.

To further compare the three schemes, the simulated schemes were compared statistically by computing the max, mean, and median values of the corresponding schemes for different parameters of evaluation. With respect to the AODV algorithm, the results are shown in Table 7-1. The values indicate the relative accuracy of the simulation output.

Table 7-1: The statistic for route discovery

Route discovery vs. pause time			
Improvement Ratio (Reduction)			
Pause Time	**HARP1**	**HARP2**	**HARP3**
0	93.24%	81.08%	50.77%
50	93.29%	73.39%	51.11%
100	92.18%	92.94%	46.63%
200	89.32%	92.15%	57.72%
300	88.00%	90.68%	64.29%

500	85.94%	91.17%	86.82%
Max	**93.29%**	**92.94%**	**86.82%**
Mean	**90.75%**	**86.90%**	**59.55%**
Median	**90.75%**	**90.92%**	**54.41%**

Route discovery vs. speed

Improvement Ratio (Reduction)			
Speed	**HARP1**	**HARP2**	**HARP3**
10	94.39%	77.23%	56.38%
20	97.21%	64.94%	53.76%
30	97.38%	66.25%	61.86%
40	97.84%	70.59%	65.05%
50	98.53%	75.79%	69.72%
60	98.79%	79.25%	75.97%
Max	**98.79%**	**79.25%**	**75.97%**
Mean	**97.36%**	**72.34%**	**63.79%**
Median	**97.61%**	**73.19%**	**63.46%**

Route discovery vs. Network size

Improvement Ratio (Reduction)			
Network size	**HARP1**	**HARP2**	**HARP3**
10	56.53%	66.51%	18.63%
30	87.05%	86.54%	49.76%
50	92.82%	55.42%	41.16%
60	94.80%	53.60%	52.30%
70	97.74%	80.23%	58.47%
Max	**97.74%**	**86.54%**	**58.47%**
Mean	**85.79%**	**68.46%**	**44.06%**
Median	**92.82%**	**66.51%**	**49.76%**

7.2.2.2 The efficiency of data packet delivery

Figures 7-5, 7-6 and 7-7 show the efficiency of the proposed schemes that is represented by the ERDP against mobility with different pause time, node speeds, and network size. In general, as can be seen in these figures, the ERDP in these schemes is higher than the

ERDP of AODV in terms of different values of pause time, speeds and different number of nodes. This means that fewer control packets are needed to deliver data packets from source to destination, due to the long-lived route established by using HDA.

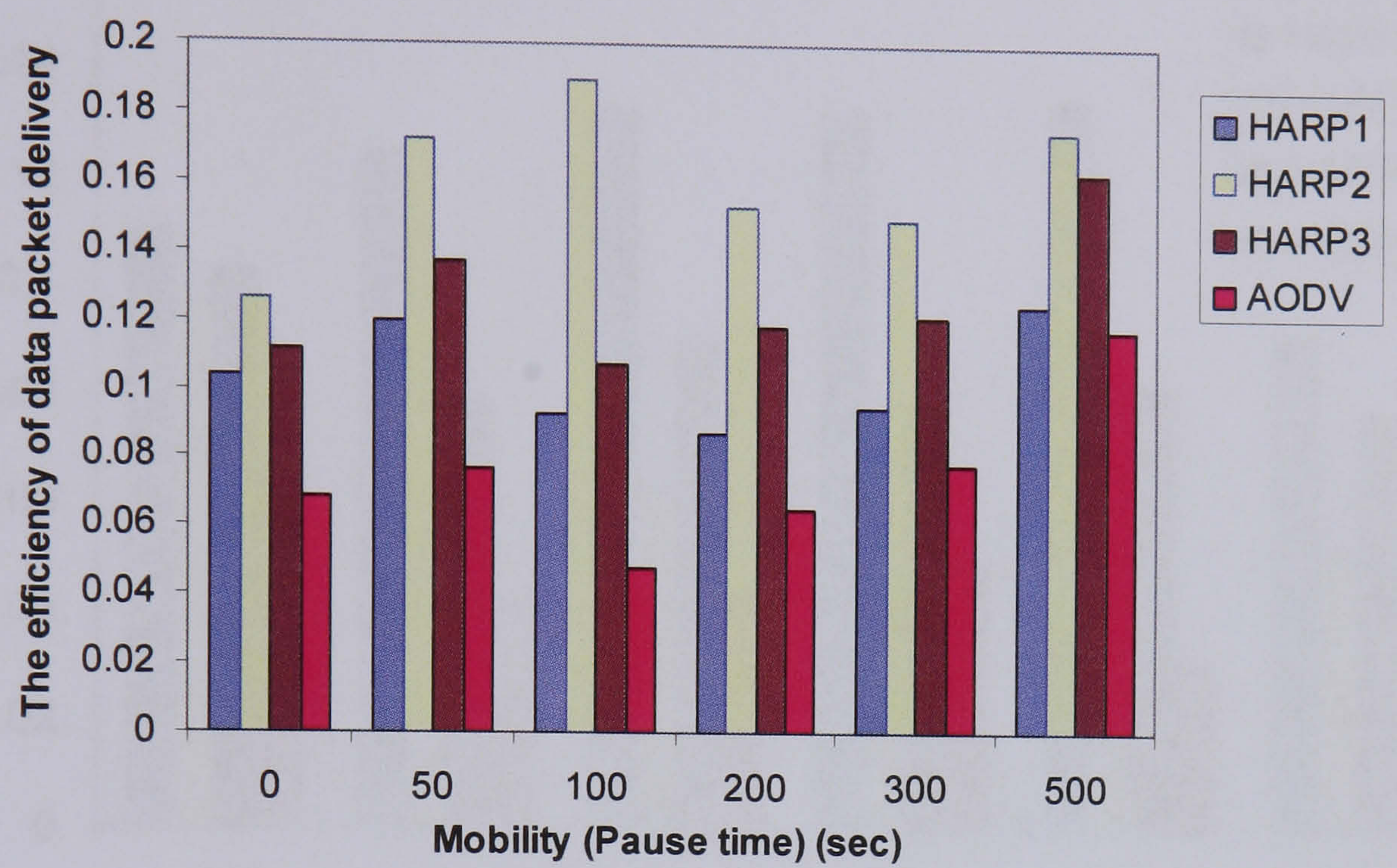


Figure 7-5: The efficiency of data packet delivery vs. Mobility (pause time)

Figure 7-6 depicts the ERDP ratio against the speed of mobile nodes. As can be seen in this figure at low speeds (10-20m/s), in AODV, HARP2 and HARP3, the ERDP is decreased. At higher speed (>20m/s), HARP2 and HARP3 show good efficiency as the ERDP ratio is approximately constant.

Analysing the scalability of the network with the number of mobile nodes, Figure 7-7 compares the ERDP ratio against number of nodes. When the number of mobile nodes increases from 10 nodes up to 30 nodes, the ERDP ratio for all schemes decreases sharply. After 30 nodes, the ERDP becomes for all proposed schemes nearly constant, while it continues decreasing for AODV. This indicates that all the proposed, schemes after a limited number of nodes, are hardly affected by the increased number of nodes. The ERDP ratio for AODV, however, continues to decrease as the number of nodes is increasing. This indicates that a higher number of nodes in ad hoc network leads to a higher number of nodes which will contribute to the formation of the route. This causes to higher probability of link breaks and thus, more control packets needed to repair or re-establish broken routes.

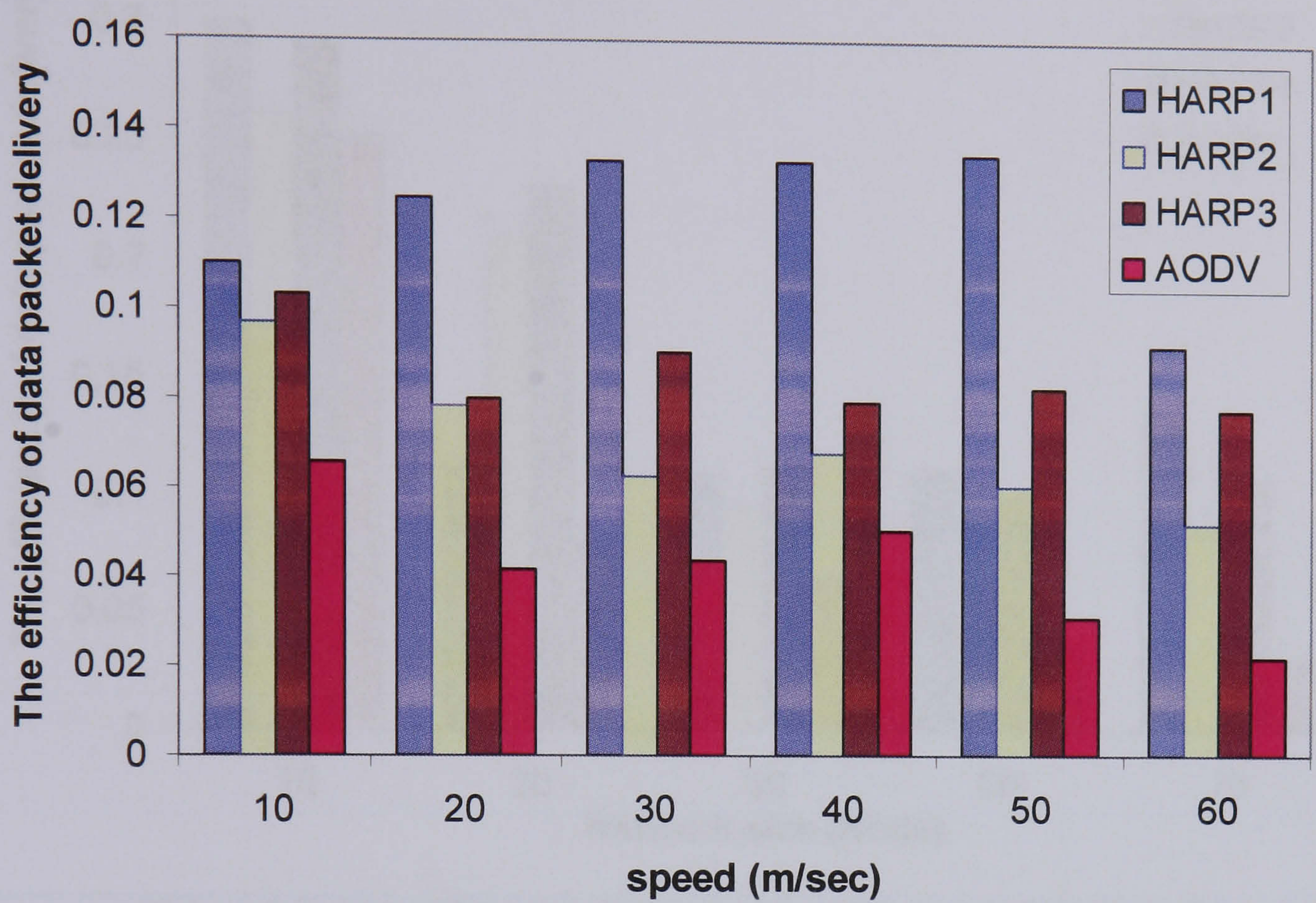


Figure 7-6: The efficiency of data packet delivery vs. peed

The maximum, mean, and median values of the corresponding schemes for different parameters of evaluation are shown in Table 7-2. With respect to the AODV, the values, again, indicate the relative accuracy of the simulation output.

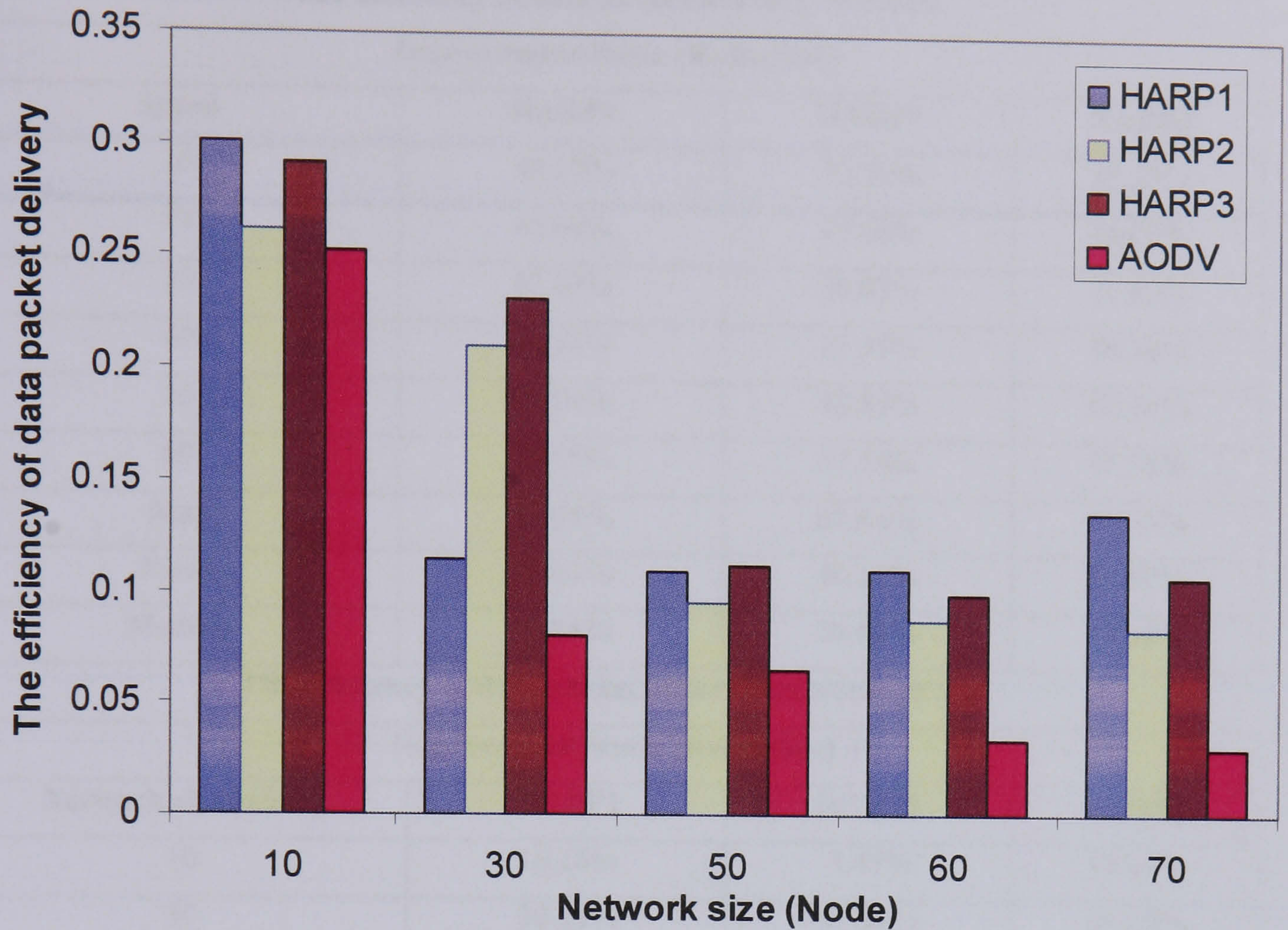


Figure 7-7: The efficiency of data packet delivery vs. Network size

Table 7-2: The statistic for the efficiency of data packet delivery

The efficiency of data packet delivery vs. pause time			
Improvement Ratio (Reduction)			
Pause Time	**HARP1**	**HARP2**	**HARP3**
0	33.97%	45.42%	38.29%
50	35.83%	55.23%	43.94%
100	48.89%	74.94%	55.58%
200	25.75%	57.54%	44.92%
300	17.85%	47.67%	35.32%
500	5.72%	32.79%	27.84%
Max	**48.89%**	**74.94%**	**55.58%**
Mean	**28.00%**	**52.27%**	**40.98%**
Median	**29.86%**	**51.45%**	**41.11%**

The efficiency of data packet delivery vs. speed

Improvement Ratio (Reduction)			
Speed	**HARP1**	**HARP2**	**HARP3**
10	40.19%	32.29%	36.23%
20	66.66%	47.08%	48.00%
30	67.02%	30.03%	51.60%
40	62.01%	25.35%	36.50%
50	77.04%	48.83%	62.49%
60	76.09%	57.54%	71.76%
Max	**77.04%**	**57.54%**	**71.76%**
Mean	**64.83%**	**40.18%**	**51.10%**
Median	**66.84%**	**39.68%**	**49.80%**

The efficiency of data packet delivery vs. Network size

Improvement Ratio (Reduction)			
Network size [node]	**HARP1**	**HARP2**	**HARP3**
10	16.16%	3.45%	13.58%
30	30.29%	61.86%	65.35%
50	40.19%	31.58%	41.83%
60	69.26%	60.83%	65.80%
70	78.21%	63.98%	72.32%
Max	**78.21%**	**63.98%**	**72.32%**
Mean	**46.82%**	**44.34%**	**51.78%**
Median	**40.19%**	**60.83%**	**65.35%**

7.2.2.3 The Average end-to-end delay

As mentioned before, by utilising and adopting the flooding technique used by some routing algorithms such as AODV, it is more likely to find the required path in a short time with an acceptable delay at the expense of significant overhead, collisions, and without guarantee to select the path that will last for acceptable period. However, in most applications, it is crucial and important to find the path that lasts longest with reduced overhead and collision and with an acceptable level of delay.

The comparison between the proposed schemes in terms of the average end-to-end delay of transferred data packets against mobility with different pause time, nodes speeds and number of mobile nodes are depicted in the Figures 7-8, 7-9 and 7-10. In these figures, it can be seen that the proposed schemes have an increased delay compared to the fully flooding technique protocol, AODV. This is because the proposed schemes reduce the flooding effects by only forwarding the route request packets to a few selected nodes. Therefore, additional delays will be occurring during establishment of the path to the destination. When the speed of mobile nodes is increased, the average end-to-end delay is slightly increased in HARP2 and HARP3 as shown in Figure 7-9. This is because there is a higher probability of link breaks caused by increasing the speed of nodes.

In terms of scalability of network with the number of nodes, HARP3 shows better performance among other schemes for equal or more than 30 nodes, as shown in Figure 7-10. This is due to the availability of a higher number of neighbouring nodes to select from as a next hop which are close to the destination. In AODV, the end-to-end delay is nearly constant when the number of nodes is higher than 30. This is due to the transmission storm caused by the contribution of all nodes in the network in flooding the route request packets, which in turn reduces the delay of finding the route to the destination. Nevertheless, this is on the cost of heavy overhead of control packets, which consume the bandwidth used by the network.

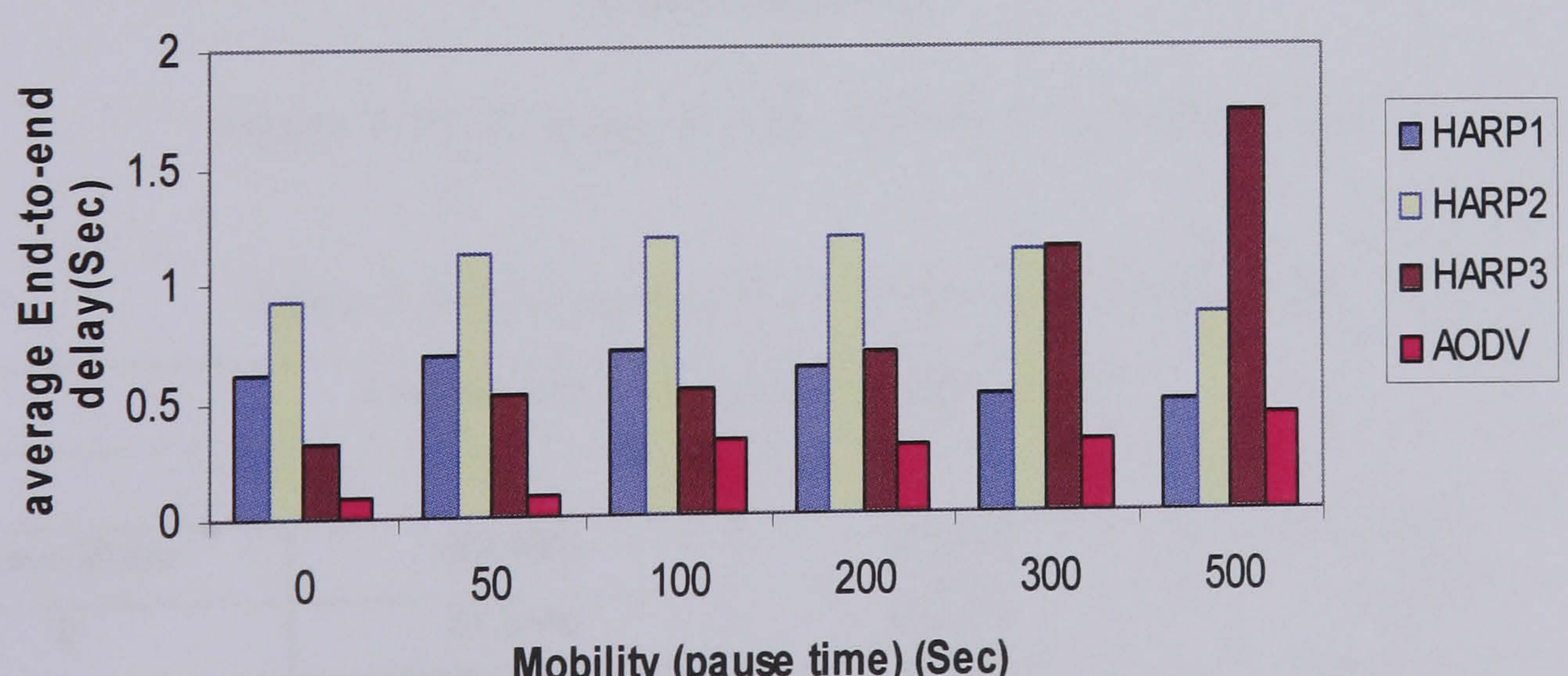


Figure 7-8: Average End-to-end delay vs. Mobility (pause time)

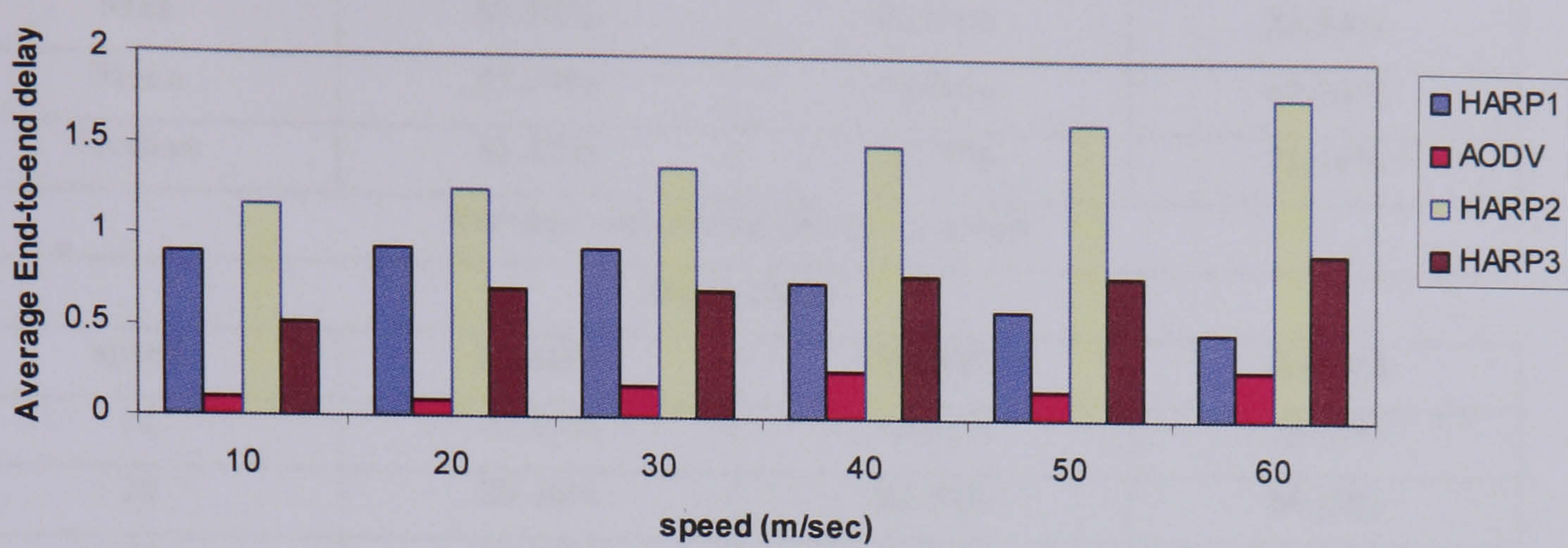


Figure 7-9: Average End-to-end delay vs. speed

The maximum, mean, and median values of the corresponding schemes for different parameters of evaluation are shown in Table 7-3. With respect to the AODV algorithm, the values indicate the relative accuracy of the simulation output.

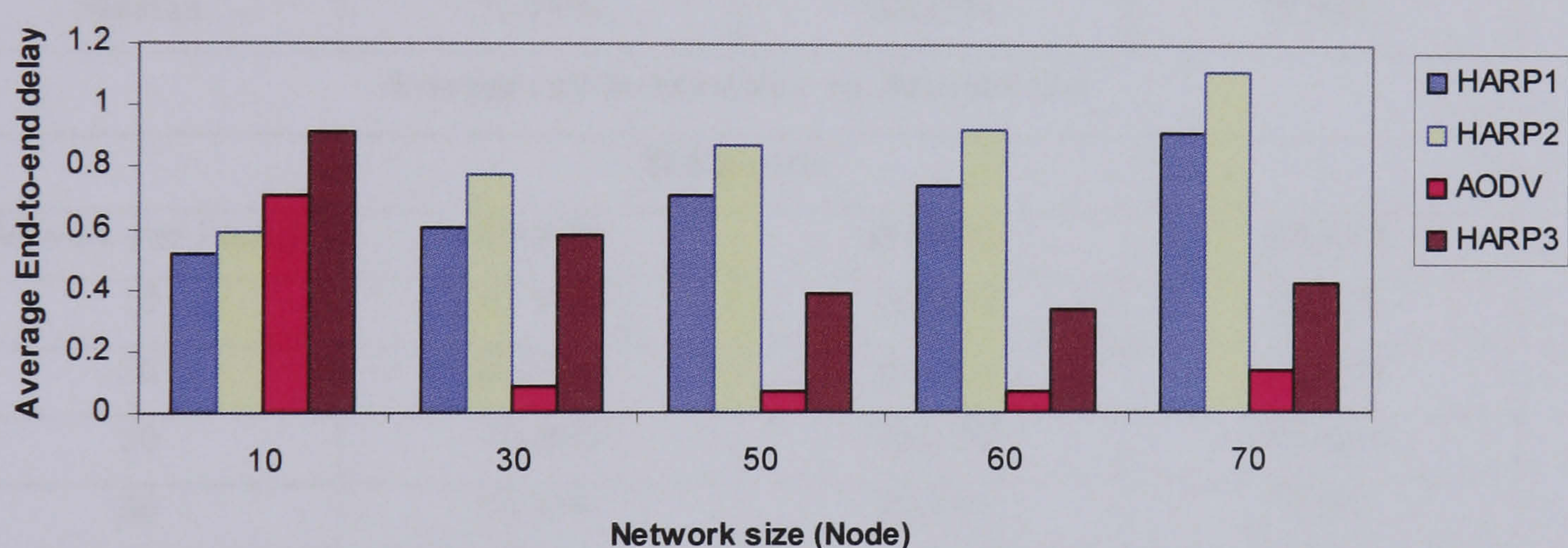


Figure 7-10: Average End-to-end delay vs. Network size

Table 7-3: The statistic for Average end-to-end-delay

Average end-to-end-delay vs. pause time			
Delay ratio			
Pause Time	**HARP1**	**HARP2**	**HARP3**
0	85.35%	90.22%	72.74%
50	87.76%	92.35%	83.84%
100	55.12%	73.11%	40.74%
200	53.82%	75.42%	57.97%
300	37.77%	72.15%	72.54%
500	12.55%	50.12%	75.72%

Max	**87.76%**	**92.35%**	**83.84%**
Mean	**55.39%**	**75.56%**	**67.26%**
Median	**54.47%**	**74.27%**	**72.64%**

Average end-to-end-delay vs. speed

Delay ratio			
speed	**HARP1**	**HARP2**	**HARP3**
10	87.85%	90.65%	78.71%
20	89.66%	92.39%	86.49%
30	80.58%	86.96%	74.29%
40	65.62%	82.78%	67.46%
50	72.99%	89.98%	79.14%
60	44.40%	84.82%	70.66%
Max	**89.66%**	**92.39%**	**86.49%**
Mean	**73.52%**	**87.93%**	**76.12%**
Median	**76.79%**	**88.47%**	**76.50%**

Average end-to-end-delay vs. Network size

Delay ratio			
Network size [node]	**HARP1**	**HARP2**	**HARP3**
10	-37.70%	-20.97%	22.27%
30	86.10%	89.13%	85.42%
50	90.46%	92.24%	82.66%
60	90.45%	92.34%	79.02%
70	85.00%	87.70%	67.50%
Max	**90.46%**	**92.34%**	**85.42%**
Mean	**62.86%**	**68.09%**	**67.37%**
Median	**86.10%**	**89.13%**	**79.02%**

7.3 Discussion and Observation

In this chapter, a comparative analysis of the proposed routing algorithms was introduced. HARP1, HARP2 and HARP3 have been compared between each other and the AODV routing protocol. These routing protocols have been evaluated by using the most popular network simulator used by most of ad hoc researchers, which is the NS-2. A comparison of results show that the three schemes clearly have a significant reduction in terms of the cost of route discovery control packets (overhead) in comparison with the AODV (Table 7-1) and that these schemes are less affected by mobility, speed and number of nodes than AODV in terms of the efficiency of data packet delivery (Table 7-2).

It has been noticed, however, that in all the proposed schemes, the average end-to-end delay compared to AODV is a disadvantage for these schemes. In spite of this limitation, in many applications, finding the path that lasts longest with reduced overhead and collision and with an acceptable level of delay is crucial and important and of course, this acceptable delay is application dependant.

In terms of route discovery, at pause time less than or equal to 50 sec, HARP1 has shown better performance over HARP2 and HARP3, while at pause time higher than 50 sec, HARP2 has shown better performance over HARP1 and HARP3. HARP1 has shown better performance in route discovery against speed over the other two schemes and then HARP2 has shown better performance over HARP3. Regarding to the number of nodes, HARP1 has shown better performance in route discovery over the other two schemes, and HARP2 has shown better performance over HARP3.

In analyzing the ERDP, in terms of pause time, HARP2 has shown better performance over the other schemes, then HARP3 and HARP1 respectively. HARP1 has shown better performance in route discovery against speed over the HARP2 and HARP3, followed by HARP3 and HARP2 respectively. Regarding to the number of nodes, HARP3 has shown better performance in route discovery over the other two schemes, and HARP2 has shown better performance over HARP1. However, Table 7-4 shows which HARP algorithm has shown better performance over the others. HARP3 can be seen to be a protocol suitable for use in networks that require a very good QoS.

Table 7-4: Performance comparisons of the proposed algorithms

The scheme that shows better performance	Pause Time	Speed	Network Size
Route Discovery	<= 50 sec HARP1	HARP1	HARP1
	>50 sec HARP2		
ERDP	HARP2	HARP1	HARP3
Average End-to-End Delay	<= 100 HARP3	<=30 m/s HARP3	<30 nodes HARP1
	>100 HARP1	>30 m/s HARP1	>=30 nodes HARP3

Beyond the results for any particular scheme, two overall trends in this study are clearly visible. The first trend is that the less dependent on flooding behaviour a protocol is, the better it appears to perform in terms of overhead and efficiency of data packet delivery. This can be seen when the proposed schemes were compared with the completely flooding protocol, AODV. The second trend is that, protocols perform better if they are able to reduce the number of nodes that must react to a topology change and contribute in establishing the route between the source and the destination nodes.

Chapter 8

Adaptive Location Service for Geographical-based Routing Protocol

In this chapter, a new Adaptive Centralised Location Service (ACLS) is presented, which tracks mobile node locations. ACLS is an adaptive centralised location service that runs on the mobile nodes themselves without the need for any fixed infrastructure. Some nodes in the ad hoc network consider themselves as location servers according to their location and situation in the network. Each mobile node periodically updates the location servers with its current location. Nodes that are not servers send their position updates to location servers. This transmission is achieved by only knowing the expected location of the servers without knowing the actual identities of these servers. The update message is assisted by predefining the location of the origin centre of the servers. Queries for a mobile node's location also use the predefined the location of the origin centre of the servers to find a location position for that node. The identity of the receiver (server) is *a priori* unknown to the initiator of the message. This is called **anonymous addressing** because the receivers decide on their own, based on current values of the node's parameters and on the contents of the message, whether they are the intended destination. Mostly the position of nodes determines whether they are the destination of a message. Details about the complete idea are coming next in this chapter.

8.1 Motivation

With the growing popularity of outdoor locating devices (e.g., GPS) it is both technically and economically feasible for a mobile device to know its physical location. In mobile ad hoc networks, the communication between nodes goes through intermediate nodes. This, therefore, requires the packet to be forwarded from the source to the destination nodes bypassing the intermediate nodes. The packets could be efficiently forwarded by intermediate nodes with aid of the location information.

Many proposed routing protocols for mobile ad hoc networks rely on geographical information for forwarding packets to the final destinations such as Location-Aided Routing (LAR) [1, 14], Zone-Based Hierarchical Link State (ZHLS) [15], Flow Oriented Routing Protocol (FORP) [16], and Greedy Perimeter Stateless Routing (GPSR) [17, 18]. Generally speaking, this type of routing protocols has three assumptions:

(1) The mobile node knows its location, which can be obtained by the aid of outdoors and indoors locating devices (e.g. GPS);
(2) The mobile node knows the location of its neighbours, which can be achieved by periodical exchange of HELLO beacon including the location information;
(3) The source knows the location of the destination in advance, which is the role of the location service routing protocols.

First of all, it is necessary to define the "*location-based*" routing and the "*location service*" in order to show the difference between them. Location-based routing algorithms use location information to forward packets from the source to the destination. A location service is combined with and used by location-based routing algorithms to provide the source with the location information for the required destination in a mobile ad hoc network. The sender then includes in the packet's destination address the provided position of the destination. The location service can be described as a mechanism for a node to track the location of other nodes in the network topology.

The proposed algorithm, HARP3, is one of the location-based routing protocols, and needs a location service mechanism to provide the destination location. Therefore, a new adaptive location service is proposed in this chapter in order to overcome some of the drawbacks that accompany the existing location service algorithms. With the comparison with other existing location service approaches, the main objectives of the proposed location service are:

- Reducing the time spent on looking for a server that has information about the position of a required node since the server locations in this approach, unlike the existing approaches, is known by all nodes.
- Reducing the path length from a requester node to a server node.

- Find solution for the two types of failure caused by node mobility which occurs in most already existing location service approaches. These failures are:
    - A location server may have out-of-date information, which this proposed approach solves by using different servers that are updated frequently. Using more than one server in the network minimises the probability of a server being unavailable and hence, minimises the probability of using expired location information.
    - A server may move out of its current location. In this approach, moving a server out of the servers' pool does not have any effect on the overall functionality of the algorithms. This is because the algorithms always try to make available more than one server in the pool by expanding the pool area, as will be explained later in this chapter.

8.2 Preliminary Work on Location Service

In location services, the service has to be responsive to the mobility of nodes. When a node moves, its position changes and the service must be updated according to the mobility pattern. In addition, the task of location services usually is to provide the requester with the position of the requested node. Hence, in order to communicate with the requested node, a geographical routing approach should be employed.

In fact, there are three approaches adopted for a possible design of a location service:

1. Using flooding across the whole network to get nodes locations: Mobile nodes broadcast their location information throughout the MANET periodically. So the source knows the up-to-date location of the destination before data transmission.
2. Central static location server: In which a server is located in one position in the network and all other nodes request the position of requested nodes from this static server.
3. Every node acts as server for a few others: Each node is responsible for keeping and tracking the position change of a small number of nodes in the network.

Location services can also be classified according to how many nodes host the service or how many nodes act as a server in the network. In this classification, four classes are available:

I) Some-for-some: in which some nodes act as servers for some other nodes.
II) Some-for-all: in which some nodes act as servers for all nodes in the network.
III) All-for-some: such as each node maintains a routing table for all nodes within two hops.
IV) All-for-all: in which each node maintains the position of all other nodes in the network.

There is a number of existing location service approaches that need to be examined before continuing research in this field.

8.2.1 Distance Routing Effect Algorithm for Mobility

The Distance Routing Effect Algorithm for Mobility (DREAM) [25] is a flooding-based location service than can be considered to be a proactive method. Each node periodically broadcasts a control packet containing its own coordinates with respect to the specific positioning system considered. The routing table stored at each node contains location information for any other node in the network. In DREAM, the closer nodes are updated more frequently than faraway nodes. The disadvantages of this approach are:

- Excessive flooding messages are used to broadcast the position information across the networks.
- As a result of the above disadvantage, DREAM consumes significant bandwidth due to the heavy packet flooding across the network.

8.2.2 Quorum-Based Location Service

Quorum-based location service [91] is a some-for-some scheme and originates from information replication in databases and distributed systems where some nodes are chosen to form a backbone network. These backbone nodes are further divided into several quorums such that the intersection of every pair of quorums is non-empty. When a node changes its position, it sends its updated location to one subset containing the nearest backbone node. Each source node then queries the subset containing its nearest backbone for the location of the destination, and uses that location to route the message. The mechanism used in quorum-based protocols is that all nodes in the network agree upon a mapping that associates each node's unique identifier to one or more other nodes in the network. These nodes will be servers for that node where periodical location updates will be sent to and stored into as well as where location queries will be routed to. In other words, the quorum of location servers updated on each location change needs to intersect the quorum of location servers consulted in with a lookup.

The main drawbacks of this mechanism are:

- Heavy computation is required in selecting the backbone and heavy searching is needed for a node that belongs to the backbone to enquire about the location of a node.
- The movement of a backbone node will result in the reallocation of the entire backbone and the topology of the backbone will need to be rearranged.
- The possibility of disconnection of the backbone node from the network.

8.2.3 Grid Location Service

Grid Location Service (GLS) [56, 107] is an all-for-some, hierarchical location service that is built upon a number of location servers distributed throughout the network. GLS divides the ad hoc network area into many small squares. The smallest square is called a first order square. Every four adjacent first order squares make up a bigger second order square, and so on (Figure 8-1).

Each mobile node keeps providing the other nodes available in the same first order square with its up-to-date location. Every mobile node recruits one node as its server from each of four (n-1)-order squares (n > 1) to keep its location information. Selecting the server is done by selecting the node with the least greater node ID in each (n-1)-order square. GLS has three main activities: location server selection, location query request, and location server update.

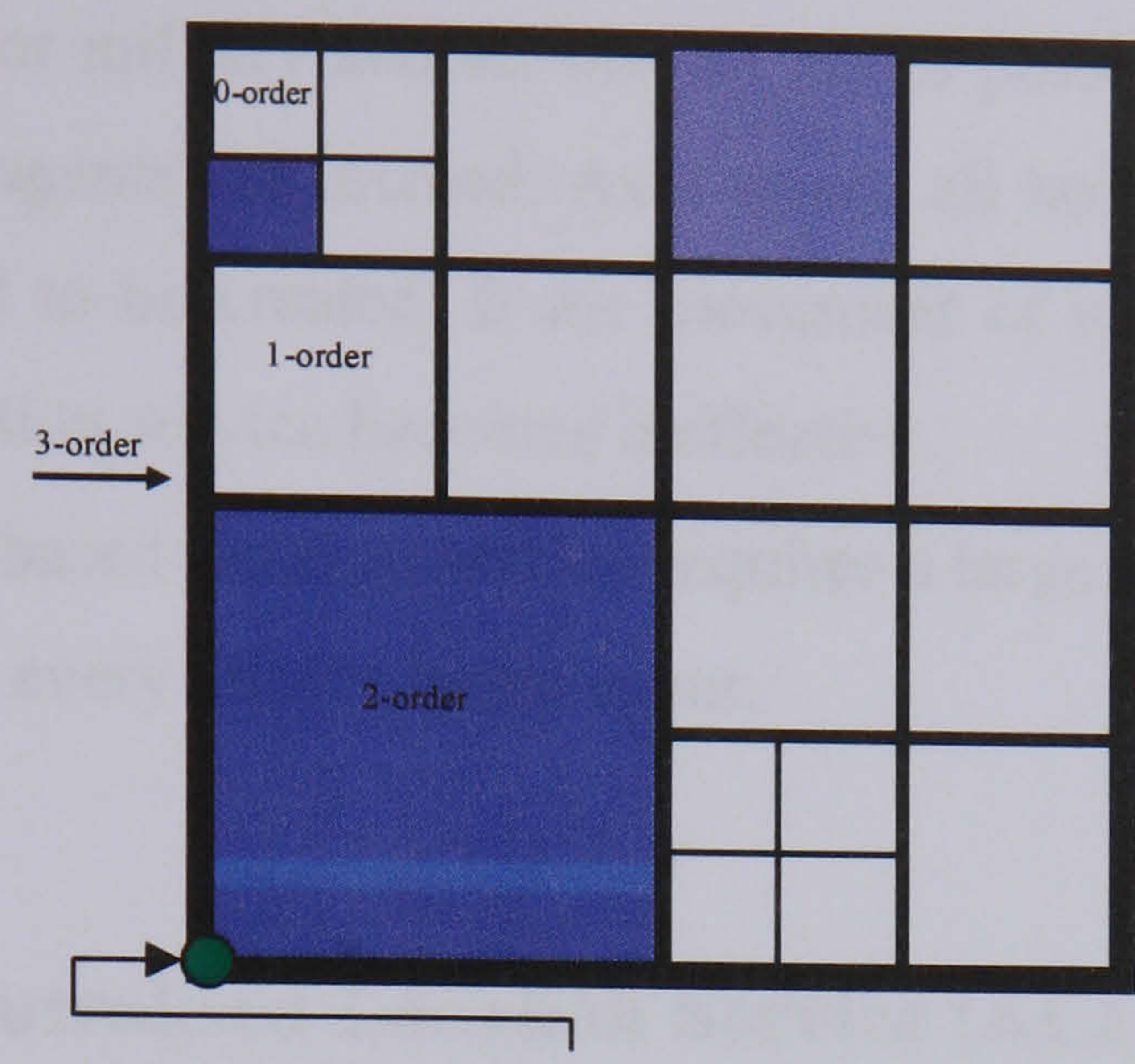


Figure 8-1: GLS's spatial hierarchy

The main drawbacks of GLS are:

- The heavy computation of selecting the location of servers for each node, the location query request, and location server update in different grid levels and different distance between the node and its servers, which are some of them in faraway grid.
- A node that is acting as a server for other nodes may move out of its current grid. This causes a server failure.

8.2.4 Home Agent-based System

The Home Agent-based System [108] is all-for-some location service scheme. It uses a home agent based strategy for location updates and destination searches. Each node chooses a certain circular area which is the location scope where it first joins the MANET as its home agent. It subsequently sends its location update messages to all the mobile nodes in its home agent. Each node in the network broadcasts its position to neighbouring nodes. Since the location of home agent is transmitted to all the other nodes at the beginning, queries about the position of this node can be sent to its home agent and get the corresponding reply. The drawbacks of this scheme are:

- The inefficiency. When the node moves far away from its home agent, location updates have to go across a long distance. In addition, in some scenarios such as rescue missions or military actions that all nodes possibly move out of the region where all home agents are located. As a result, all homes become ineffective and new homes need to be created. If the movement of nodes is intensive, the home agent-based location service becomes ineffective.

- The home agent-based location service requires a large amount of memory as every node has to keep every other's home agent.

8.3 Adaptive Centralised Location Service (ACLS)

The main properties of a location service that will guarantee the scalability in the following senses are:

- To spread the maintained location service information evenly over many nodes to guarantee the availability of this information in case of failure of any node that maintains the information.
- The failure of a node should not affect the reachability of other nodes.
- The location information storage and the cost of communication of the location service should grow as a small function of the total number of nodes.
- The time of searching for a location of node should be as low as possible.
- The availability of up-to-date location service at any time.

With all these in mind, a new Adaptive Centralised Location Service (ACLS) has been developed that satisfies all of these requirements. ACLS is divided into four main activities:

1) Location Server Selection
2) Location Server Update
3) Location servers information exchange
4) Location Query Request

Initially, the area covered by the ad hoc network is arranged into a number of concentric circles of increasing diameter size (Figure 8-2).

All nodes agree on the global origin of the concentric circles. The size of smallest diameter of smallest circle is r = R/2, where R is the transmission range of a node. The diameter size of circles is increasing by r.

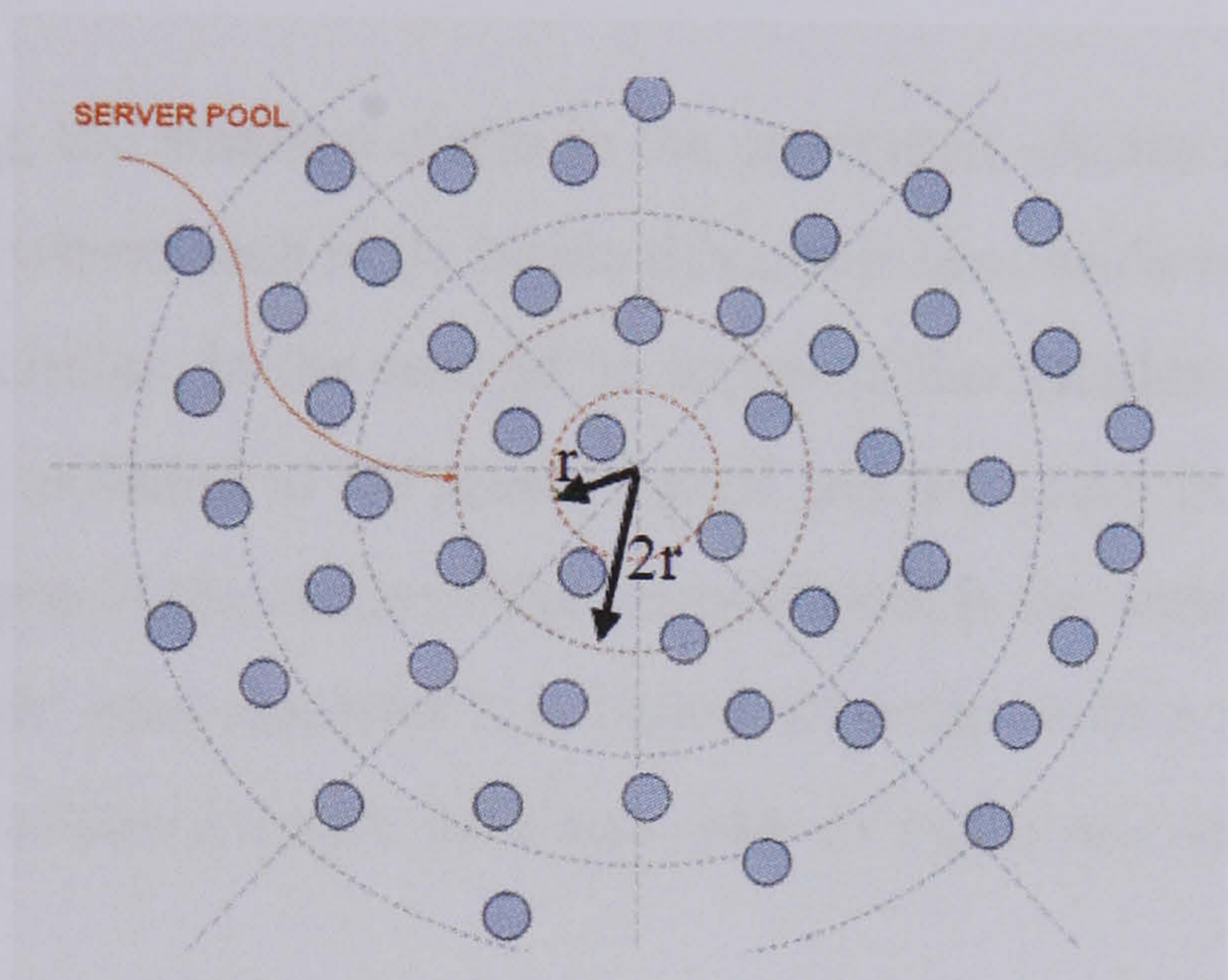


Figure 8-2 ACLS's spatial network

The assumption that all nodes agree on the global origin coordinate of the concentric circles is similar to GLS. GLS considers the bottom left hand side point of the network area is a global origin agreed by all nodes.

One way to know the global origin by a node joined the network recently could be:

- Either by giving the global origin coordinate to every node manually before joining the network, and this will take some time to setup the devices before using them.
- By giving the global origin coordinate to one node (master node) manually before joining the network, and when a node joins the network, it floods the network using a small beacon packet to enquire about the global origin. When the becaon reaches to the master node, the master node replies with another small beacon packet to inform the requested node about the global origin.

These two above approaches require control over the devices by a network manager. For example, operations that usually involve the saving of life, or prevention of injury by a rescue group in known area such as Search And Rescue (SAR). SAR is an operation mounted by emergency services whish take the control over the devices used by them in area such as mountains, desert or forest, or at sea. Another example can be in urban situations when young children or senile people wander away from their homes. The search will be around the homes, and homes will be the origin coordinate.

8.3.1 Location Server Selection

In the very beginning, the smallest circle in the concentric circles network is considered to be a servers' pool, where each node inside this circle is considered to be a server for all other nodes in other circles. In the case of no server in the smallest circle, the next circle to the smallest one is included to the server's pool and the nodes in these two circles will be servers. For example, if the circle of the servers' pool is the smallest circle in the area, this means that servers' pool diameter is *r,* hence, all nodes with a geographical distance, d_n , from the centre of the network area less than or equal to *r* consider themselves as servers. Formally:

$$f(d_n) = \begin{cases} (d_n \leq r) & \textit{status of node is a server} \\ \\ (d_n > r) & \textit{status of node is a normal node (not server)} \end{cases}$$

The probability of a node to be a server can be calculated using Binomial distribution.

Each node checks its status periodically, if the node is inside the smallest circle, it will change its status from normal node to server node and start receiving the location update messages from other normal nodes (if any message is arrived). In addition, it will exchange the location information of nodes with other servers. Any node coming inside the servers' pool will change its status to a server, and any node leaving the servers' pool will change its status to a normal node and in the next interval time, it will delete the location information stored in the location table that was received when the node was a server.

In general, in the binomial distribution with the number of mobile nodes, *n,* and probability, *p,* of a node to be a server, the probability of getting exactly *k* servers to be available in the servers' pool is given by the probability mass function:

$$f(k;n,p) = \binom{n}{k} p^k (1-p)^{n-k} \tag{7}$$

For $k = 0, 1, 2, \ldots, n$

Where
$$\binom{n}{k} = \frac{n!}{n!(n-k)!} \tag{8}$$

is the binomial coefficient "*n choose k*". The formula can be understood as follows: we want *k* successes (p^k) (servers) and $n - k$ failures $((1-p)^{n-k})$ (not servers). Figures 8-3 and 8-4 show the Binomial distribution with different number of nodes and different values of *p.*

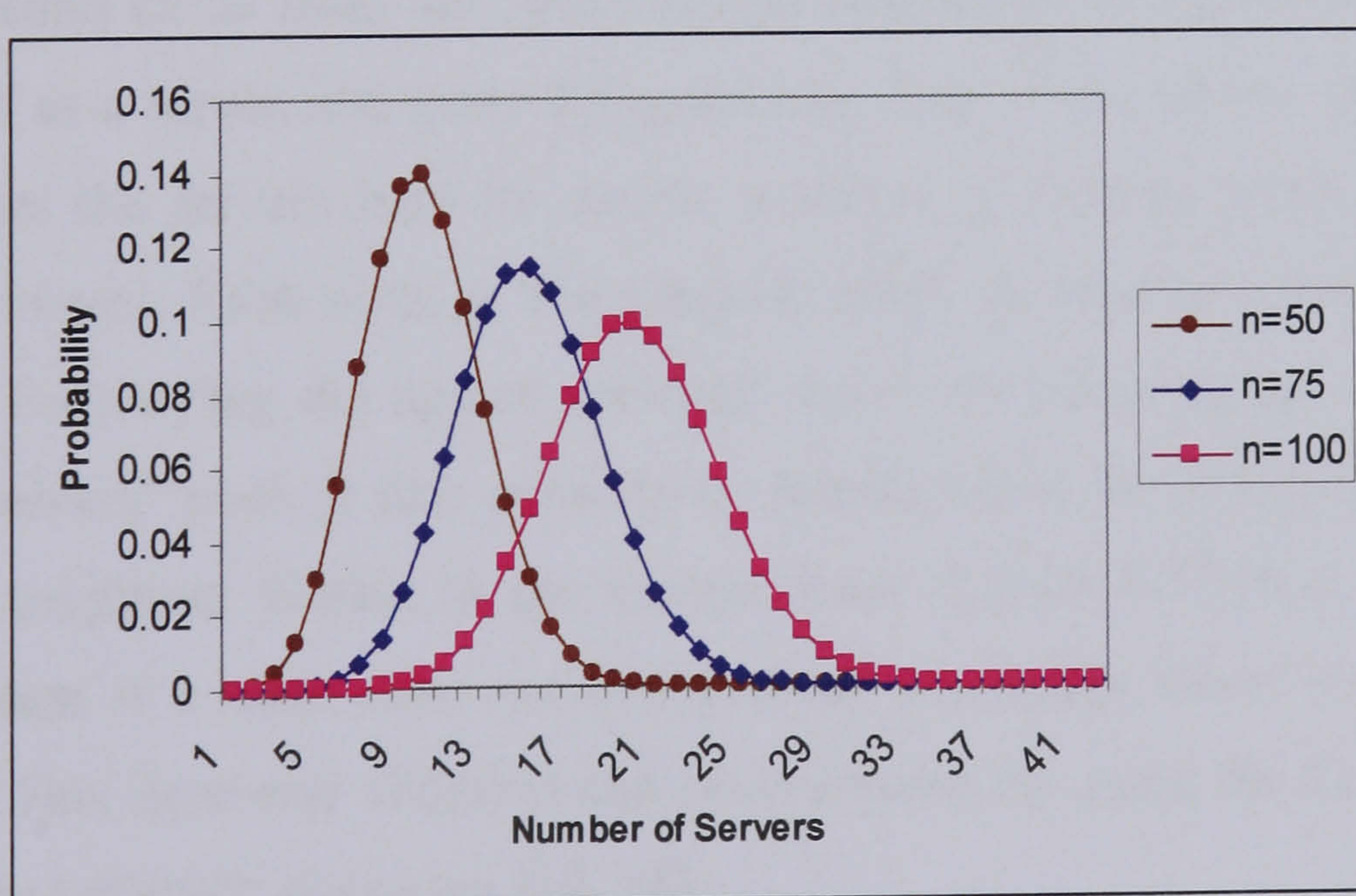


Figure 8-3: Binomial distribution for $p = 0.2$

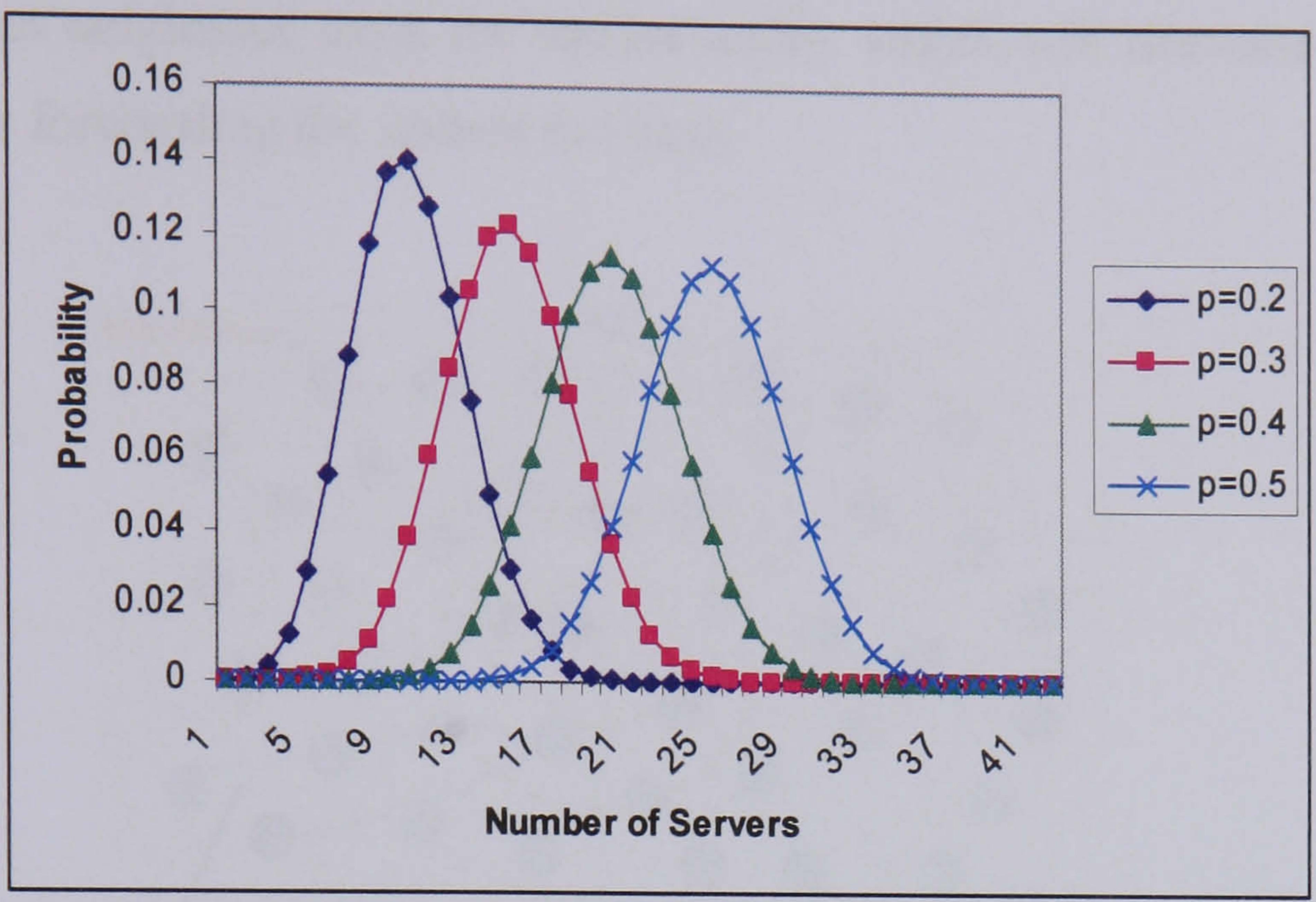


Figure 8-4: Binomial distribution for $n = 50$

8.3.2 Location Server Update

Each mobile node in the ad hoc network sends its location information to its neighbour's nodes in an interval time. This is not only useful for knowing the neighbours locations, but it is also useful in determining the size of the servers' pool. For example, when a node in the second circle from the centre has no neighbours in the first circle, the node considers itself as a server and starts doing the task duty of the server. Each node in the network updates the servers with its current position. A location server update occurs when a node moves. Each node in the network sends an Update Message toward the servers' pool. Forwarding the update message occurs by selecting the next hop that is closer to the servers' pool. It first consults its routing table and chooses to forward the packet to the neighbour closest to the servers' pool (Figure 8-5).There is, however, a potential problem if a node does not know about any nodes closer than itself to the servers' pool. This dead-end situation can be overcome by using the Greedy Perimeter Stateless Routing (GPSR) algorithm [17, 18].

The update message does not require a reply message nor a long life of the link between the sender and next hop since the sender needs only to hand the update message off to the next hop. Therefore, for optimisation, the closest neighbour to the servers' pool is selected (farthest neighbour from the sender node), which will decrease the number of hops needed for forwarding the update message.

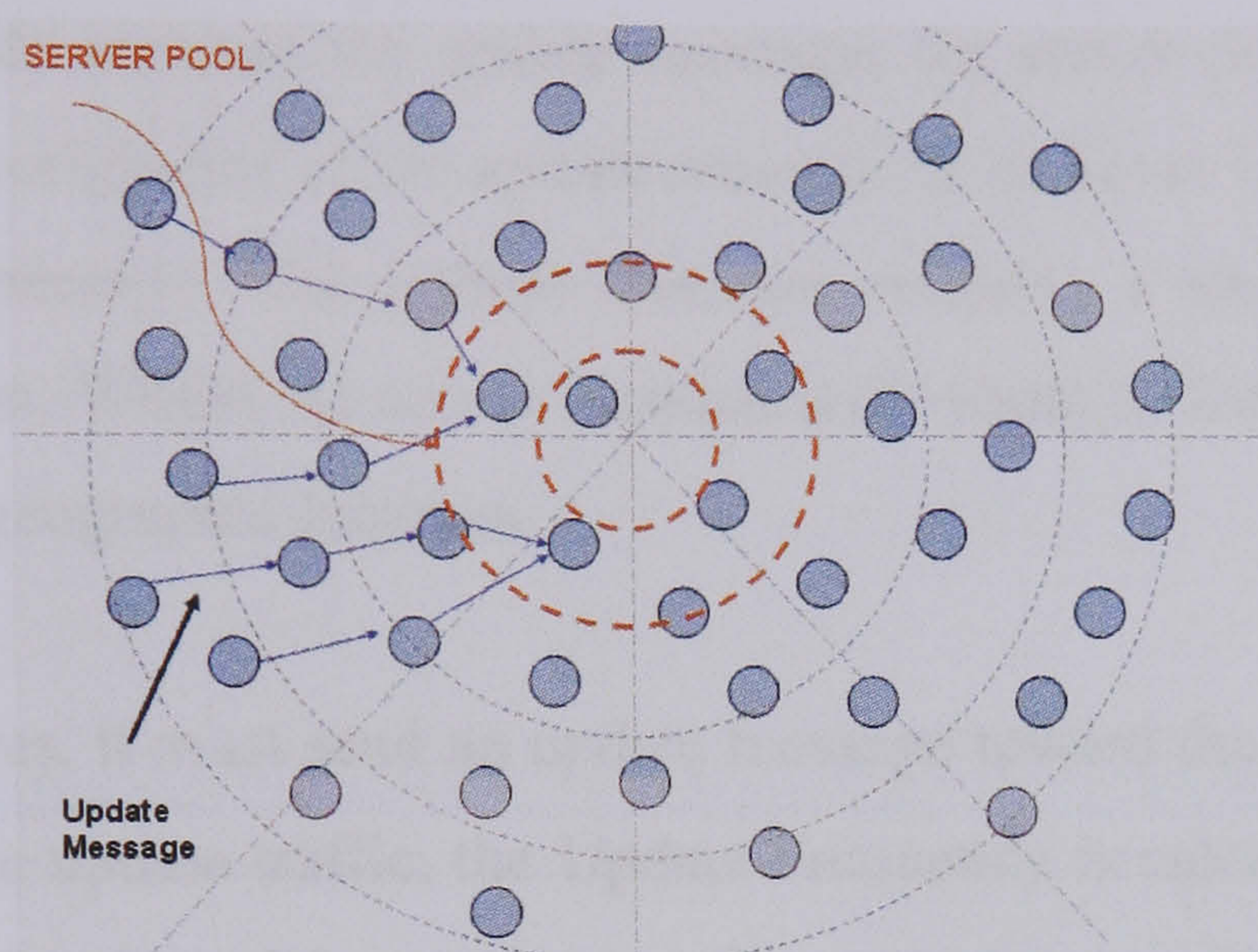


Figure 8-5: ACLS's spatial network

Formally, given P is the set of nodes in the network, then a node g of a subset neighbours S of P is the nearest neighbours of S if $s \leq g$, for all neighbours s of S. If the function of selecting the next hop toward the servers' pool is $f(NextHop)$ and the distance between the sender and the centre point of the servers' pool is d_{s_sp} and the distance between a neighbour to the sender and the centre point of the servers' pool is $d_{en's}$ then, the selected neighbour satisfies:

$$f(NextHop) \Rightarrow \begin{cases} \max\left|(d_{n\_sp1}, d_{n\_sp2}, \ldots d_{n\_spS})\right| = 0 \ , d_{n\_sp} < d_{s\_sp} & apply\ GPSR \\ \\ \max\left|(d_{n\_sp1}, d_{n\_sp2}, \ldots d_{n\_spS})\right| > 0 \ , d_{n\_sp} < d_{s\_sp} & Neighbour\ available \end{cases}$$

The identity of the receiver (server) is *a priori* unknown to the initiator of the location server update message because destination of this message is unknown. This is called **anonymous addressing** because the receivers decide on their own based on the current values of the node's parameters and on the contents of the message, whether they are the intended destination. Mostly, the position of nodes determine whether they are the destination of a message.

When a server node receives the update message, the server node updates the location information of the originator of the update message in its Sever Location Table and stops forwarding this message. The update message contains a sender node's ID and its geographic location. Whilst the server location table contains list of records containing a node's ID and its geographic location.

When a node moves, it must send an update message toward the servers' pool diametric. To avoid excessive update traffic, the Update Frequency is calculated using a Threshold Distance and the location of the node depending on the servers' pool. If the node, due to movement, comes inside the servers' pool, it changes its status to server and forwards its location information to other servers in the pool. The threshold distance is the distance the node has travelled since the last update. For example, when a node moves a distance *d*; the node then updates its location servers. In other words, a node updates its location servers at a rate proportional to its speed, and the slower nodes are updated less frequently than the faster nodes.

8.3.3 Location Servers Information Exchange

Nodes that are of type servers in the servers' pool follow the following rules:

- Each server node updates its Server Location Table information at receiving an update message.
- Each server node exchanges its Server location table with other servers inside the servers' pool by sending Server Update Message (SUM) in a periodic manner.
- The server node that received a location request message to inquiry about a location of a node has to follow the following rules:
    a. If it has the requested information in its server location table, it will send a reply toward the requester node that generates the request message, otherwise,

b. It will broadcast the received request message to its neighbours. The neighbour that is a server and has the requested information will send a reply to the requester node directly; otherwise (does not have the requested information) it will follow the same rule followed by the previous server. The node that is not a server and receives the broadcasted requested message will forward it toward the centre of the servers' pool. To stop the loop-to-infinity, a sequence number for each packet generated by the originator is used and the node that receives the packet twice will drop that packet received previously.

The Server Update Message includes the locations table of the nodes in the network, and the servers' information table. Each entry in the locations table contains a node's ID and its geographic location. Each entry in the servers' information contains a server's ID, its position, and its radius. As an optimisation, in order to reduce the size of the Server Update Message, the server that needs to send a Server Update Message only includes the updated/changed information in the server location table and the servers' information table. For example, consider the server location table of a server contains location information for five nodes. At a specific time, the server node receives an update message from one of the five nodes stored in its location table. This server, at the interval time, will initiate a Server Update Message to be sent to other servers. This message contains only the location information of the node that sent the update message, since the server itself has already sent the location information for other four nodes in previous interval time.

By exchanging the Server Update Message (Figure 8-6) the servers know each other. Each server node has a servers' information table containing information about other servers available in the servers' pool. Each entry of the servers' table is a record includes a server's ID, radius, and its geographic location.

If a server node moves out of the servers' pool, then:

- If the node was the only node in the servers' pool, then it will still operate as a server node in the next circle and propagates its information to all other nodes inside the new defined pool (including the new circle).
- Whilst if the node moved outside the servers' pool and still other servers available in the server area, the node will remove the information related to other nodes either as servers or as normal nodes (server location table, Servers' information table).

8.3.4 Location Query Request

When a node needs a location of a destination, it triggers a location query request message. The location query request message is forwarded using geographic forwarding toward the servers' pool by selecting the nodes that are closest to the centre of pool. The same as in the Location Server Update, a node may not know about any nodes closer than itself to the servers' pool. This dead-end situation is overcome by using GPSR. The location query request message includes information about the originator node (the IP address, the position, and the packet sequence id). It also includes the IP address of requested node. The originator information is used for forwarding the request reply toward the originator.

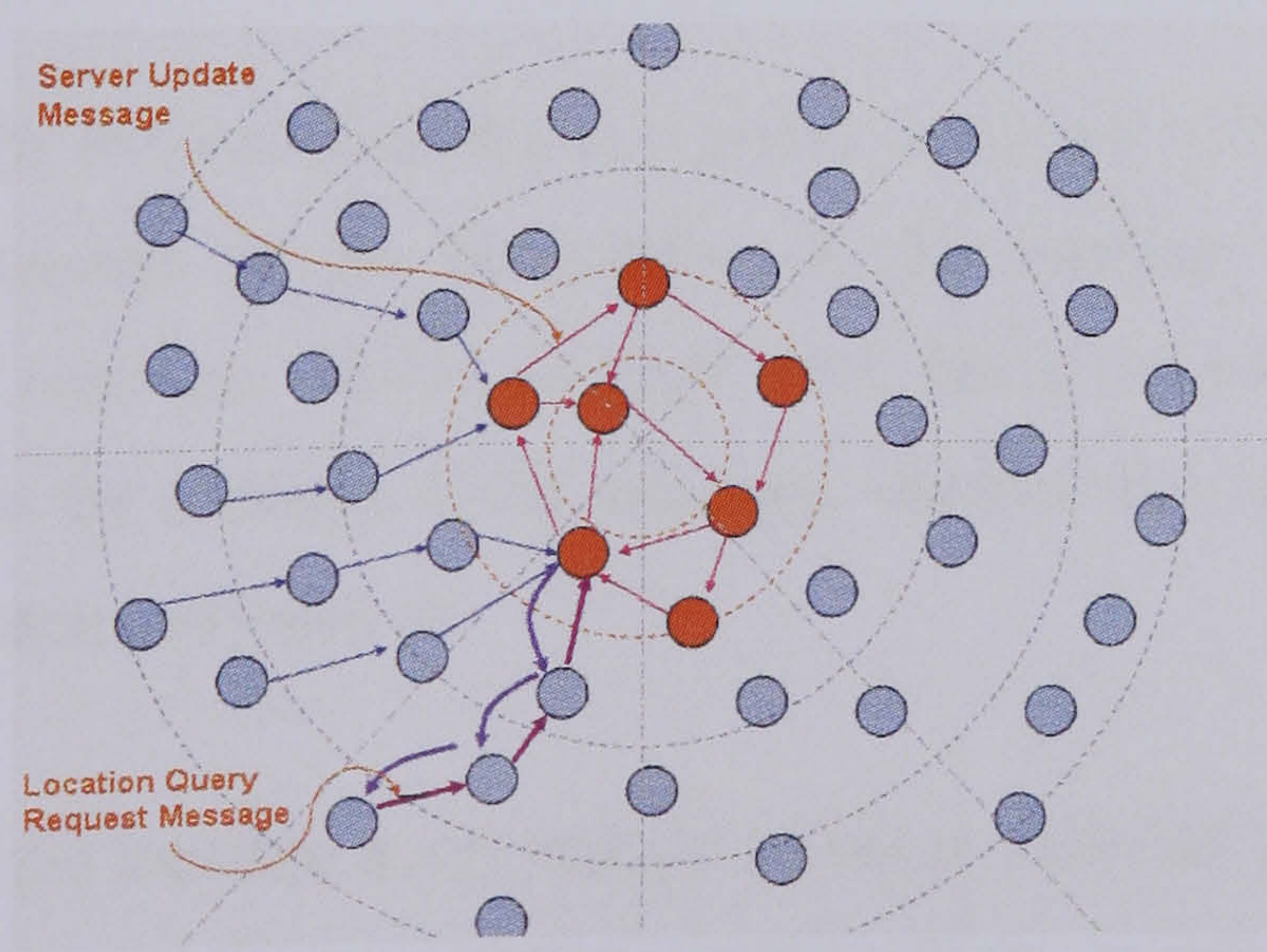


Figure 8-6: Server update and location query request messages

When one server receives the location query request message, it first updates the sender information in the Server Location Table and changes the flag of the updated record to "Updated record". This is because, at the interval time, this server will send a Server Update Message to other servers including this updated record. After that, the server checks if it has the requested location information for the requested destination, and:

a) If the location of the requested node is available in the Server location table, the server replies by sending a Location Reply message toward the sender following the same reversed path followed by the location query request message (Figure 8-6). (Another possibility is when the server receives the location query request message this server then forwards the query directly to the destination, which responds to the location query request with its most recent location), in ACLS, the first option is followed.

b) If the location of the requested node does not exist in the server location table, the server consults other servers for the requested location by flooding the request packet to its neighbours. The server that received this message and has an answer about the requested location replies directly to the originator node of the location query request message. The node that is not a server will forward the request message toward the closest neighbour to the centre.

The identity of the receiver (server) is *a priori* unknown to the initiator of the location query request message as the destination of this message is unknown (anonymous addressing). The receivers decide on their own, based on current values of the node's parameters and on the contents of the message, whether they are the intended destination or have the requested information.

The originator of the location query request message waits for a reply for a period of time (T_{LR}). If no reply is received, another request message is sent. The number of retries is limited by a number (e.g. 3 times). After that, the originator has two options: either the location query request message is flooded across the network or the destination is considered unavailable, because each node in the network is required to send its location information to the servers' pool. In the validation of the ACLS, the second option was chosen, since each node should have registered in the servers and we are trying to minimise the overhead. After receiving the reply message, the node starts sending the data packets toward the destination location.

8.4 Optimisation

Some optimisations implemented in the ACLS are summarised in the following:

- For optimisation during forwarding the update message, the closest neighbour to the servers' pool is selected (farthest neighbour from the sender node), and this decreases the number of hops needed for forwarding the update message.
- To avoid excessive update traffic, the update frequency is calculated using a threshold distance and the location of the node. The threshold distance is the distance the node has travelled since the last update.
- In order to reduce the size of the Server Update Message, the server that needs to send a Server Update Message includes in the message only the updated/changed information in the server location table and the servers' information table.
- One of the optimisations implemented in ACLS uses the expiration time of the geographical information of the destination node. This is will reduce the number of request messages sent when receiving data packets in very short time (shorter than the expiration period) for the same destination (see section 1.7.4).
- During forwarding the query request packet, if this packet meets the requested node, the requested node sends a query reply without continuing to forward the request packet toward the servers.
- During forwarding the data packet, if the packet meets a server that has fresher information about the destination location; the data packet updates the information regarding the destination in its fields. Hence, forwarding the packet will be more accurate. This is one of the advantages of using the servers in the middle of the network where most of the forwarded packets generally will pass through this area.

8.5 ACLS Advantages

Bearing in mind the above description, the essential advantages of ACLS can be summarised as the following:

1) Reducing the time needed to search for a server in order to inquire about the position of a node. In ACLS, unlike most existing location service approaches, all nodes in the network know the servers' area.
2) Reducing the path length from a node to a server node, since the inquiry request is forced toward the centre area of the network (the maximum is the radius of the network).
3) Find solutions for the two types of failure caused by node mobility, which occurs in many already existing location service approaches. These failures are:
    1. A location server may have out-of-date information. This type of failure is solved in ACLS by using different servers, which are updated frequently. Using more than one server guarantees minimising the probability of unavailability of a server and hence, minimises the probability of using old location information.
    2. A server may move out of its current location. In ACLS, moving a server out of the servers' pool does not have any effect on the overall functionality of the algorithms because the algorithm always tries to make more than one server in the pool available by expanding the pool area if needed.

8.6 ACLS Disadvantages

1. Consider that all nodes in the network are gathered inside the smallest circle (server pool). In this case, all nodes become servers and each node will have a location information table for maintaining the locations of other nodes. In addition each node will exchange its updated location information table with other servers. This case has an advantage and a disadvantage. The advantage is that each node has location information about all other nodes in the network and therefore no

need to send location query request packet to enquire about the destination node. The disadvantage is that each node has to have a location information table about other nodes which will be exchanged with other nodes.

2. Consider that most of the nodes are available on the the perimeter area (outer circles) of the network (no nodes are available in the inner circles). In this case, the server pool's area will increase to cover several circles that contain at least two servers. Therefore, for some nodes, the path length between a node and a location of servers might be not diametric.This length might be increased for these nodes as shown in Figure 8-7.

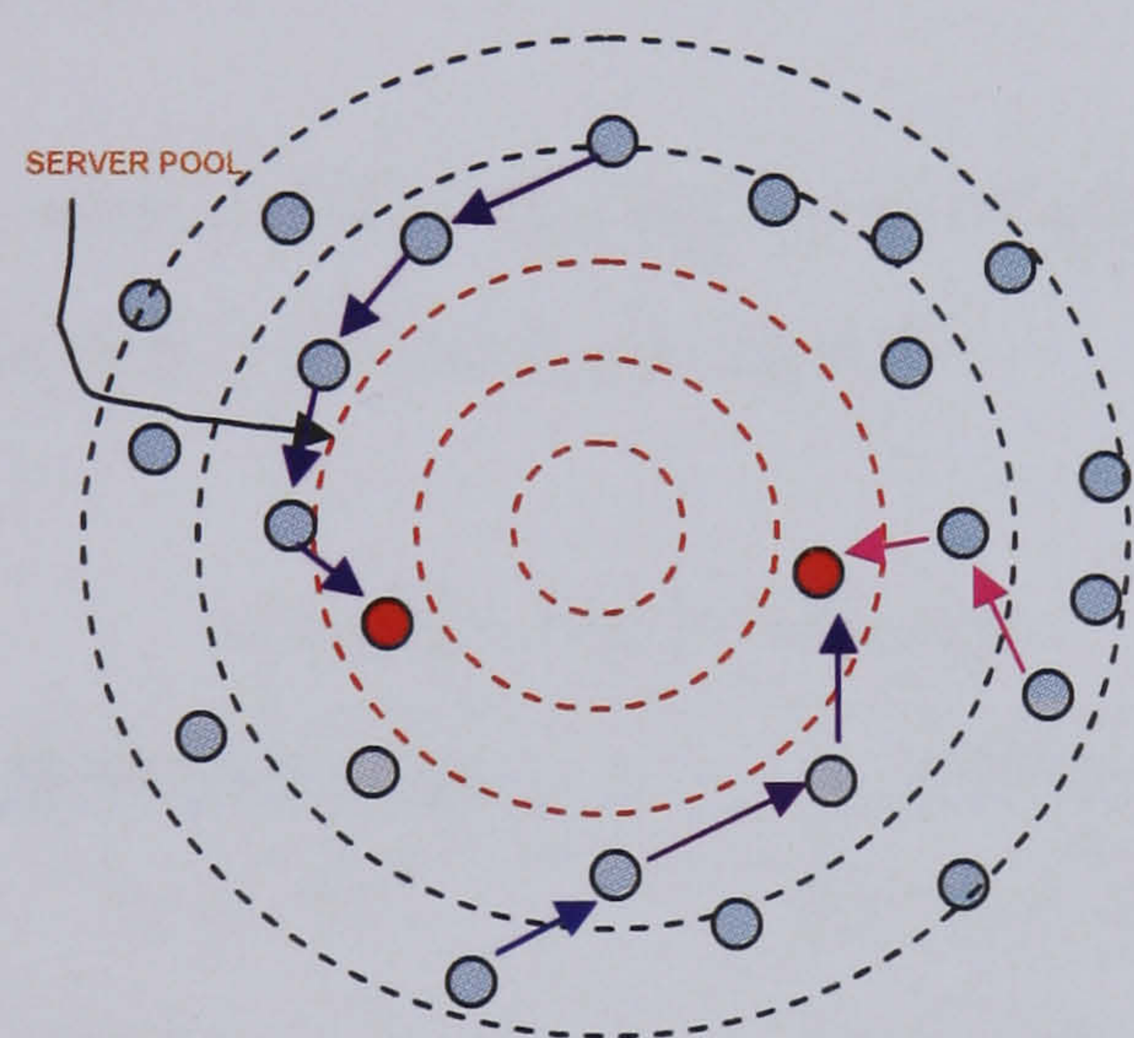


Figure 8-7: Most of the nodes are available on the outer circles

This side effect could be optimised by the following way: When a node sends an update packet to servers, each node (not a server) receiving this packet will do the following:

- Add its location informtaion to the received packet.
- Reset the interval time of the timer of its periodic location update.
- Forward the update packet to next node toward the servers.

Therefore the number of update packets is reduced as not all nodes will trigger the update location packets because it is sufficient to give another node the responsibility to pass its location information to servers on its way.

8.7 Packets/Message Format

ACLS utilises different types of packets/messages to complete the functionality of the ACLS as a location service protocol. These messages are:

- The Hello Message
- The Update Message
- The Server Update Message
- The Location Query Request Message
- The Location Reply message

8.7.1 The Hello Message

Each node in the network sends a Hello message to its neighbours. This message contains information about the node that is shown in the table 8-1.

Table 8-1: Hello Message

Hello Message	**Description**
Node ID	The node IP address
Node location	The Node position

8.7.2 The Update Message

A location server update occurs when a node moves. Each node in the network sends an Update Message toward the servers' pool. The frequency of sending the update message is controlled by the movement distance from the previous location since last updated message. The content of this message is shown in table 8-2.

Table 8-2: Update Message

Update Message	**Description**
Node ID	The Node IP address
Node Location	The Node position
Message Sequence No.	The unique Sequence No.

8.7.3 The Server Update Message

Each server node exchanges its Server location table and servers information with other servers inside the servers' pool by sending a Server Update Message in a periodic manner. The Server Update Message includes the locations table of the nodes in the network, and the servers' information table. This message includes the information shown in table 8-3.

Table 8-3: The server update message

Server Update Message	Description
The server ID	The server IP address
The server location	The position of the server
The server radius	The radius of the server
Nodes list: IDs and locations	List of nodes that its locations are updated since last server update message
Servers list: IDs, locations, and radiuses	List of servers that its information are updated since last server update message

8.7.4 The Location Query Request Message

When a node needs a location for a destination, it triggers a location query request message. The location query request message includes information about the originator node (the IP address, the position, and the packet sequence id), and include the requested node' IP address. The originator information is used for forwarding the request reply toward the originator. The location query request message includes the information shown in table 8-4.

Table 8-4: Location Query Request Message

Location Query Request Message	Description
Source ID	The source IP address
Source location	The source position
the packet sequence No.	the packet sequence id
Ultimate target ID	The Ultimate target IP address

8.7.5 The Location Reply Message

When a server receives the location query request message, the server checks whether it has the requested location information for the requested destination. If the location of the requested node is available in the Server location table, the server replies by sending a Location Reply message toward the originator of the request message. The location reply message includes the information shown in table 8-5.

Table 8-5: The Location Reply Message

Location Reply Message	Description
Source ID	The source IP address that requested location information about the target
Source location	The source location that requested location information about the target
Ultimate target ID	The destination IP address that the source requested information about it
Ultimate target location	The destination location that the source requested information about it

8.8 The Tables Used in ACLS

In ACLS, four main tables are used to maintain the information about the nodes and servers' geographical information. These tables are: the neighbours' table, the nodes' location table at the server, the servers' information table, and the destination information table.

8.8.1 The Neighbours Table

Each node in the network exchanges its geographical information with its neighbours. The exchanged information is shown in table 8-6.

Table 8-6: Neighbours table

Neighbours table	Description
Neighbour ID	Neighbour IP address
Neighbour Location	Neighbour position

8.8.2 The Nodes' Location Table at the Server

Each server receives an update message from a node, stores the geographical information about the node, which is extracted from the update message in the nodes' location table. This information is shown in table 8-7.

Table 8-7: The nodes' location table at the server

The nodes' location table at the server	Description
Node ID	The node IP address
Node Location	The node location

8.8.3 The Servers' Information Table

The servers know each other. Each server node has a servers' information table containing information about other servers available in the servers' pool. Each entry of the servers' table is a record includes a server's ID, radius, and its geographic location as shown in table 8-8.

Table 8-8: The server information table

Sever information table	Description
Server ID	The server IP address
Server Radius	The distance from the centre
Server Location	The server location

8.8.4 The Destination Information Table

The source node sends a location request message to enquire about a location of a node. The source then receives a request reply message containing the position of the requested node. The source maintains the received information about the requested node in the destination information table that contains the following fields shown in table 8-9.

Table 8-9: The destination information table

The destination information table	Description
Destination ID	The Destination IP address
Destination Location	The Destination location
The expire time	The time that this information will be expired

The time that this information will be expired is the expected time that the geographical information about the stored node will be invalid. This can be dependent on the general environment of the network. For example, if the average speeds of the nodes in the network is 10 m/s and the threshold distance is 25 m, then the expire time is set to 25/10 = 2.5 sec. After that time, if the source needs to send data to that node, it needs to send a request message to enquire about this node. This is one of the optimisations implemented in ACLS in order to reduce the number of request messages sent when receiving data packet in very short time (shorter than the expire period) for the same destination.

8.9 Experimental Design

The main objectives of these following experiments are to measure the effectivity and efficiency of ACLS algorithm in different mobile ad hoc network environments under a range of conditions, and to measure its reaction to network topology changes. To achieve these objectives, the NS-2 simulator is used.

In an attempt to generate results that would be representative of some potential, real-world scenarios, which ACLS algorithm might encounter, simulations are run with parameters values close to the available realistic values. The protocol evaluations are based on the simulation of 50 wireless nodes for some scenarios and different number of nodes varies from 50 to 200 for other scenarios. These nodes are forming an ad hoc network, moving about over an area (1km x1km) flat space for 500 seconds of simulated time.

ACLS was evaluated by using the average and minimum numbers of servers that are available at every specific time during the simulation period. In addition, the location update success rate, the location query request success rate, the CBR delivery ratio, and the average CBR delivery end-to-end delay were used for evaluating ACLS.

8.9.1 Movement Model

Nodes in the simulation move according to the Random Waypoint model [106]. A pause time value is the main characteristic of Random Waypoint scenarios. After the node reaches a destination location, it waits at that location for a period equal to pause time. By this way of movement the pause time value reflects how often nodes move during the scenario, which in turn reflects the amount of topology change (for more details about Random Waypoint model see previous chapter).

8.9.2 Communication Model

Since the aim of the simulation is to evaluate the proposed algorithm, traffic sources were chosen to be CBR sources. When defining the parameters of the communication model, it was experimented with sending rates of four packets per second, in networks containing 10 CBR sources. The size of data payload generated by the source node was chosen to be 64 bytes in all the simulation scenarios. Using more than 64 bytes such as 1024-byte packets will result in congestion, due to lack of spatial diversity. This congestion will become a problem for the algorithm and some nodes would drop most of the packets that they received for forwarding. Without loss of generality, the parameters considered in the simulation are shown in table 8-10.

Table 8-10: Simulation's parameters

PARAMETER NAME	VALUE	DESCRIPTION
Pause Time (Sec)	10	The pause time of movement
No. of Nodes (Node)	50	Number of nodes in the network
Network Area (WxH)	1000x1000	The coverage area of the network
Node Density(node/m2)	50/1000x1000	It is the number of nodes divided by the total simulation area.
Coverage Area (m2)	196,428	Coverage area is the area of the circle whose radius is the transmission distance
Avg. No. of Neighbours	9.817	Dividing the coverage area by the node density.
Servers' pool Radius (m)	125	minimum radius of server pool
D_Threshold (m)	25	The threshold distance

Center_x, center_y	500, 500	Centre of the network area
No. of Sources (Node)	10	Number of source nodes
Speed (m/s)	10	The average speed of nodes
Data Type	CBR	Type of data
Data Packet size (Byte)	64	The data packet size
Channel Capacity (Mbps)	2	The channel capacity
Packet Rate (P/Sec)	4	The rate of sending data packets per second
Transmission Range (m)	250	The transmission range of the node
No. of Location Request Retries	3	The number of resending the location request query
Simulation Time (Sec)	500	The simulation time
Hello_Interval (Sec)	1	Hello interval time
Allowed_Hello_Loss	3	Number of Hello packets allowed to be lost
Am_I_Server_Interval (Sec)	1	Checking whether the node is serve or not
Update_Loc_Interval (Sec)	1.5	Update the server interval time
Server_Update_Interval (Sec)	1	Exchange information between server interval time
Propagation Type	TwoRayGround	The propagation type

8.9.3 Verification of ACLS Simulation Models

To ensure that the implementation of ACLS algorithm inside the network simulator NS-2 was faithful to the protocol's specifications, the procedures mentioned in the previous chapter in subsection "verification of simulation models" were followed. In addition, the result files were traced manually by tracing each packet from the beginning at the originator node until reaching to the destination. The packets in trace files were also checked that they were forwarded correctly between the nodes and servers, and between the servers themselves. The packets were traced for each part of the algorithm separately. The packets generated by the location update part to update the server with the location of nodes, were traced independently. The packets generate by the query request part, were also traced separately, and the packets generated for exchanging the information between servers were traced individually, and so on.

8.10 Performance Metrics and Results

This section consists of two main parts, the performance metrics used for evaluating the performance of ACLS algorithm, and the results and analysis.

8.10.1 Performance Metrics

The following performance metrics are used for the evaluation of ACLS:

1) The average and minimum number of servers
2) The success rate of delivering the location update packets
3) The number of generated location update packets
4) The success rate of delivering the location query request packets
5) The number of generated location query request packets
6) The data packet delivery ratio
7) The average end-to-end-delay of data packet

Each parameter metric mentioned above is evaluated in different scenarios:

10) Network sizes scenario: to evaluate the performance of ACLS with different number of nodes, and to investigate its scalability with number of nodes.
11) Speed scenario: to evaluate and investigate the performance of ACLS with different values of speed.
12) Mobility scenario: this scenario shows the performance of ACLS in terms of the mobility with different pause time values.

8.10.2 Results and Analysis

This section highlights the simulation results and the analysis of the performance parameters used for evaluating the proposed algorithm.

8.10.2.1 The Average and Minimum Number of Servers

This parameter shows the average and minimum number of servers available in the network during the simulation time. Figure 8-8 (a) shows that the average number of servers increases with increasing the number of nodes in the network. Figure 8-8 (b) depicts that always there is at least a server in the network and the minimum number of servers is always greater than zero. This is due to the adaptive server pool size that increases when the number of servers reaches to zero to include other servers from the next bigger circle following to the circle of servers.

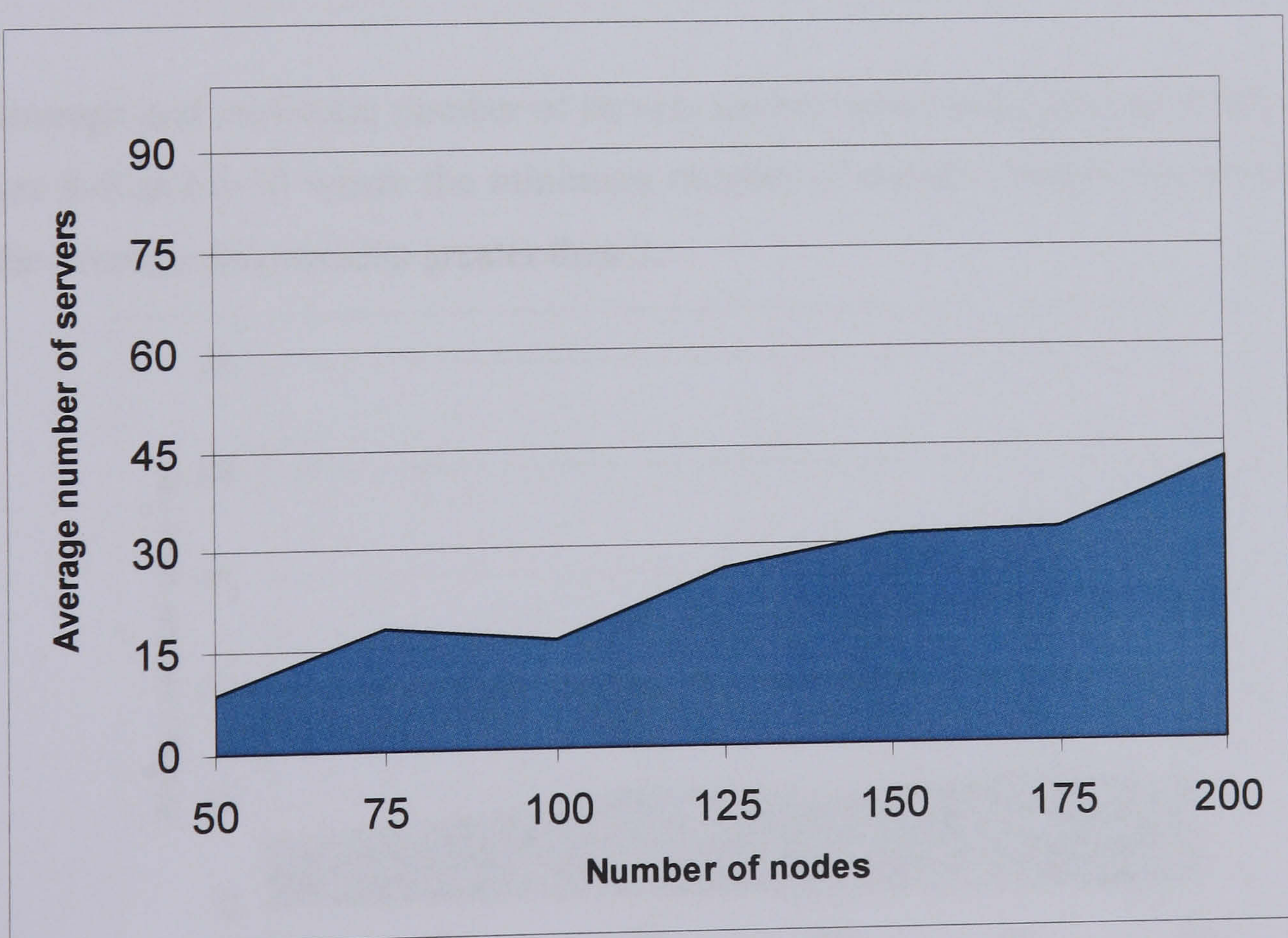


Figure 8-8: (a)

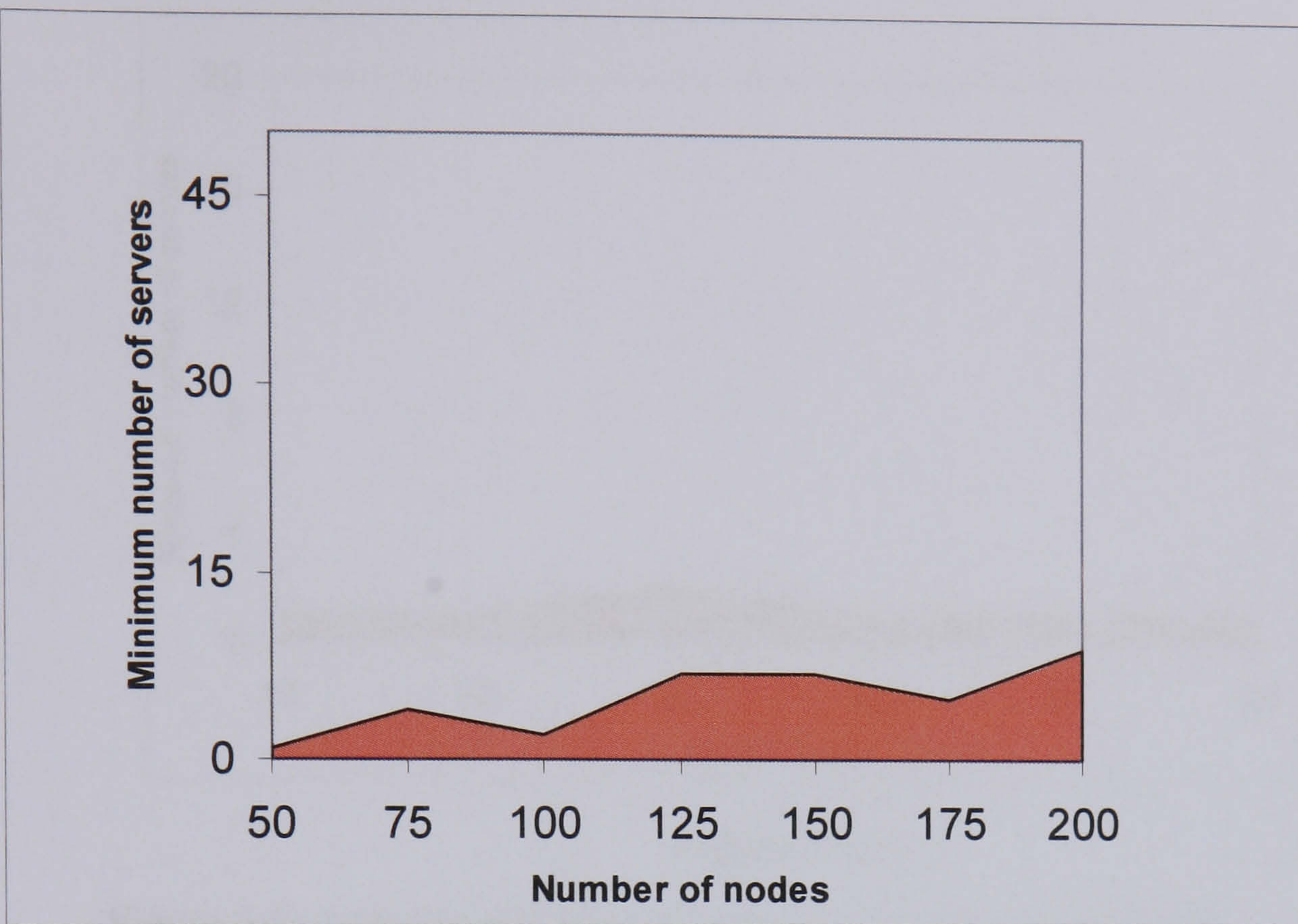


Figure 8-8: (b)

Figure 8-8: Average and minimum number of servers vs. number of nodes

The average and minimum number of servers against speed and pause time are shown in Figures 8-9 and 8-10 where the minimum number of servers remains greater than zero and the average also remains greater than 3.

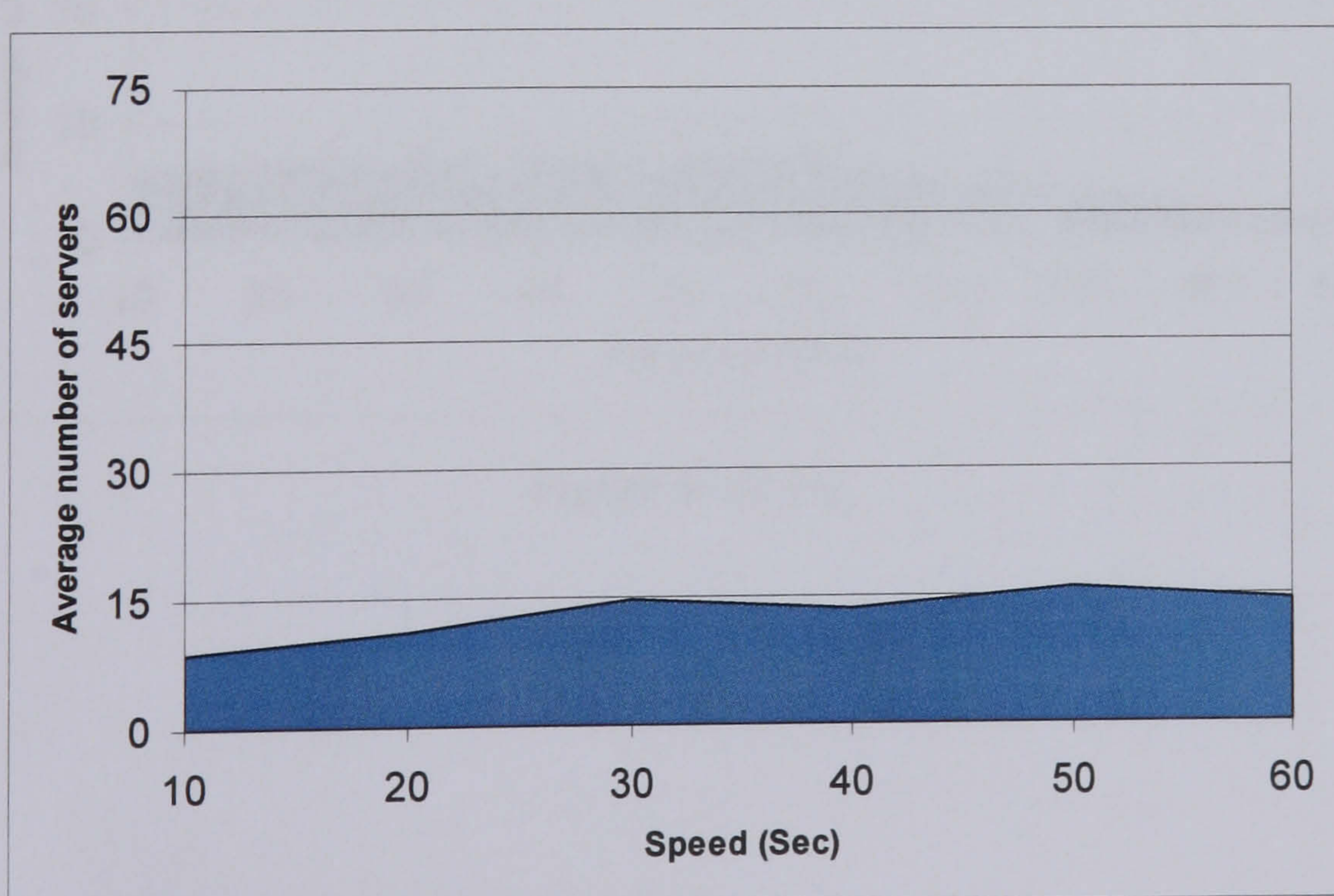


Figure 8-9: (a)

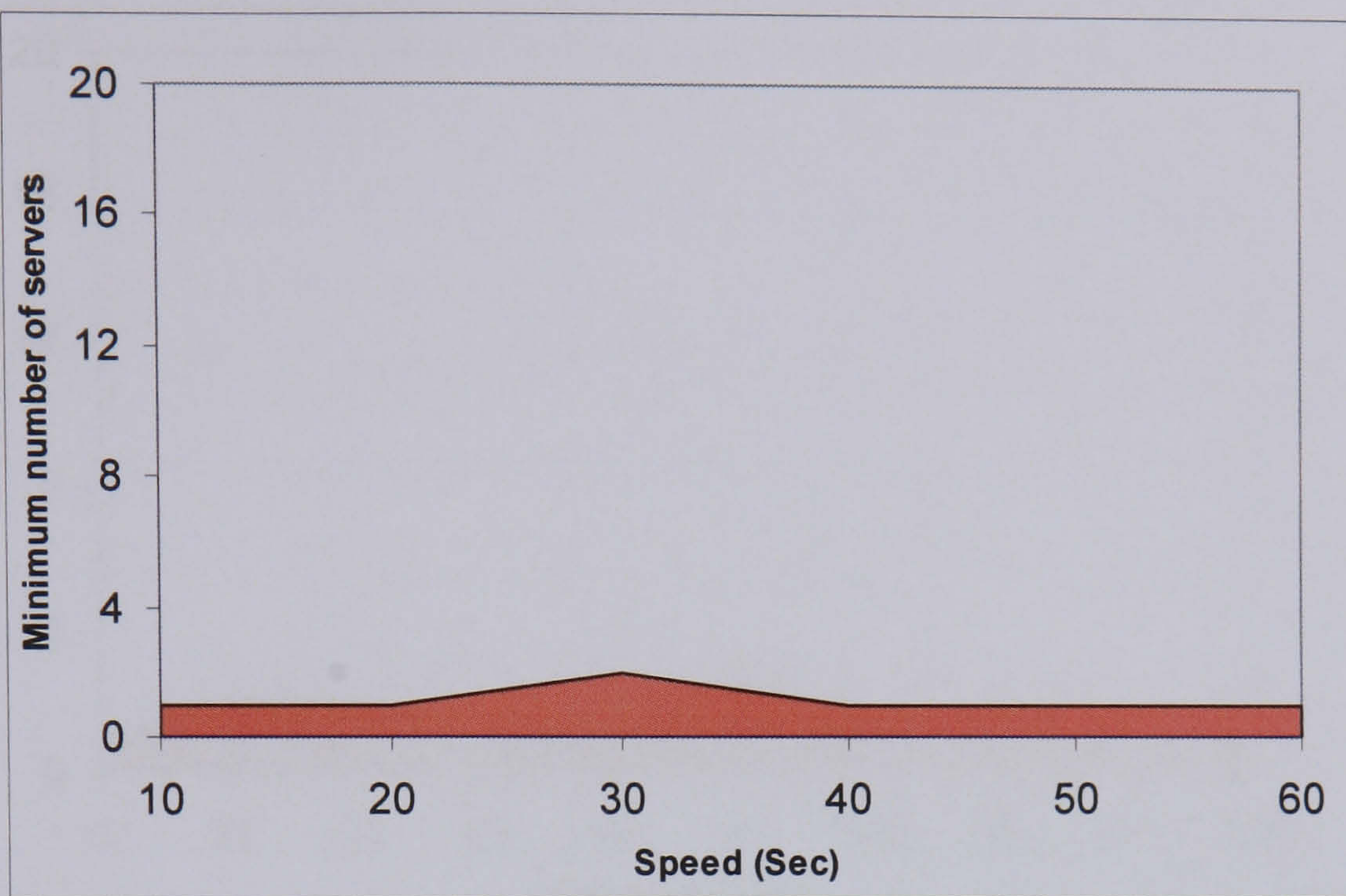


Figure 8-9: (b)

Figure 8-9: Average and minimum number of servers vs. speed

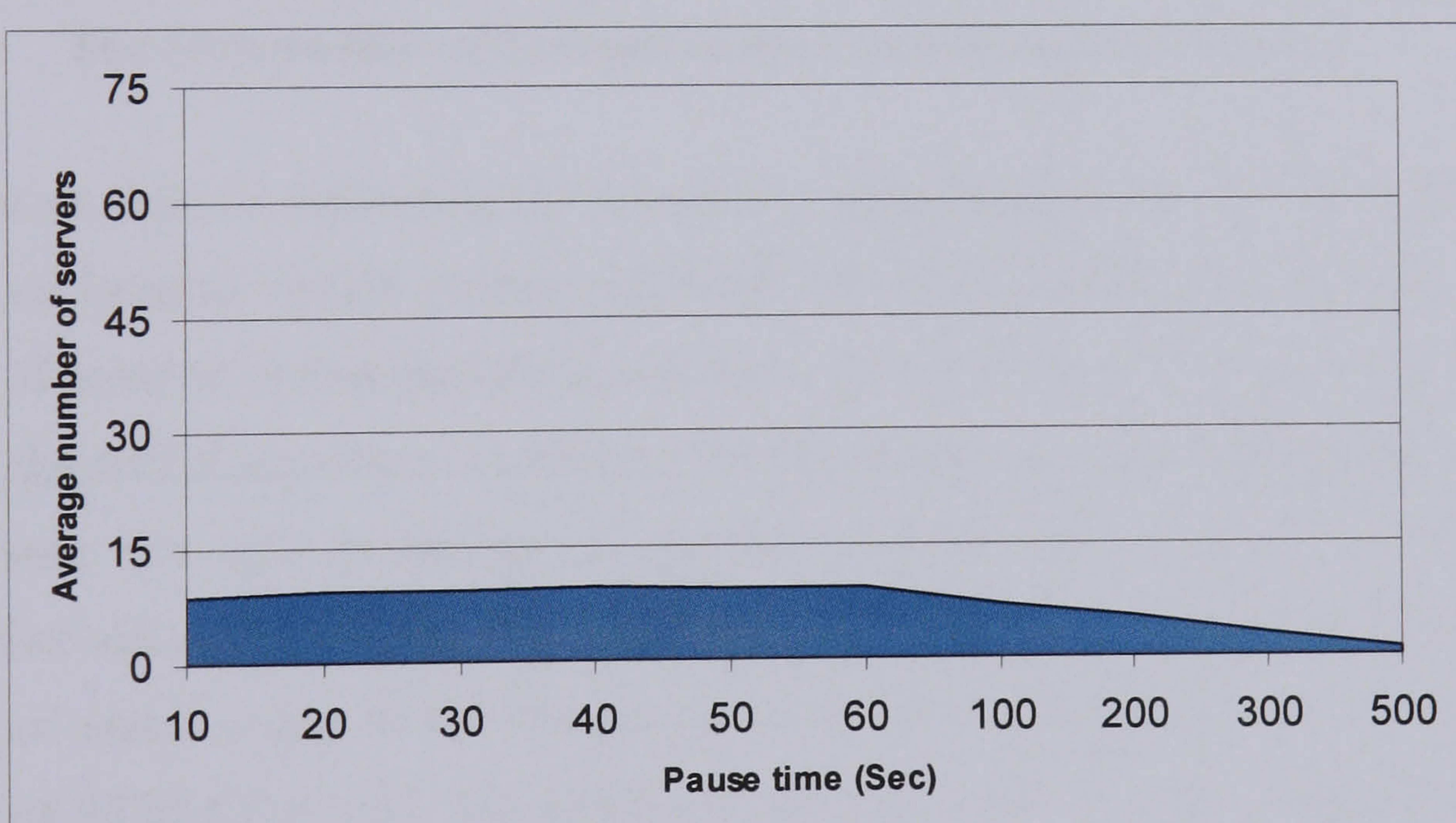


Figure 8-10: (a)

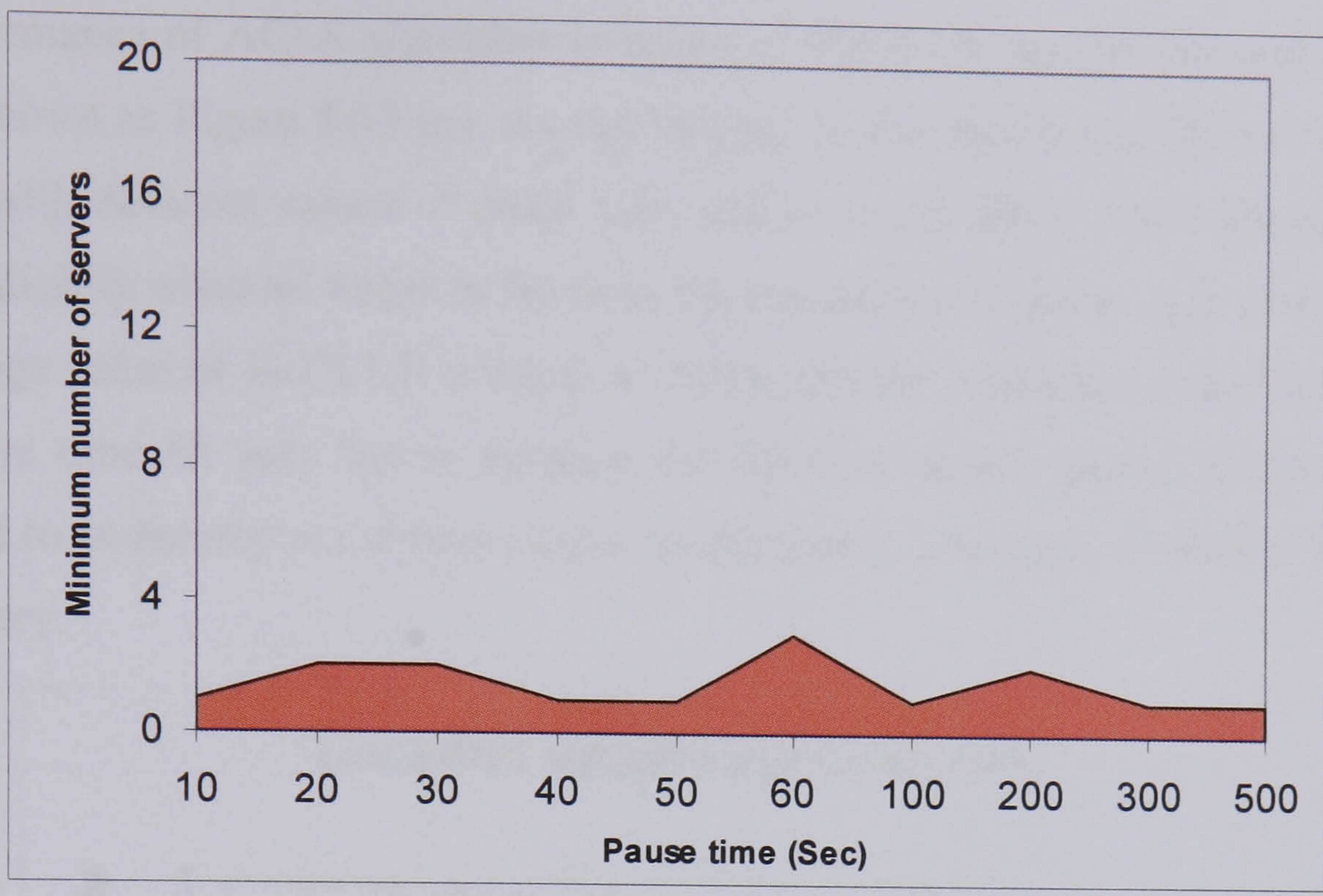


Figure 8-10: (b)

Figure 8-10: Average and minimum number of servers vs. pause time

8.10.2.2 The Success Rate of Delivering the Location Update Packets

The Success Rate of Delivering the Location Update Packets (SRDLUP) is the ratio of number of location update packets generated by normal nodes (not servers) over the number of location update packets received by servers' nodes. As can be seen in Figure 8-11 (a) the ACLS algorithm is scalable with the number of nodes joining the network. It can be seen that with increasing the number of nodes, the SRDLUP decreases very slightly but still remains above 84%. The slight reduction in SRDLUP with the increased number of nodes is due to the congestion occurred by the nodes in the network. The average of SRDLUP is 0.92. The SRDLUP rate at number of nodes equal to 50 is 0.99, which indicates that almost all location update packets reach and are received by servers.

In terms of the scalability with the speed of nodes, Figure 8-11 (b) shows that the SRDLUP rate is approximately 100% with different values of speed. The average value of SRDLUP is 0.985 and the maximum value is 0.99 at speed 10m/s. This indicates that ACLS is also scalable with the speed of nodes.

The performance of ACLS algorithm in terms of SRDLUP against the mobility (pause time) is shown in Figure 8-11 (c). As can be seen in this figure, the SRDLUP is almost constant with different values of pause time and is nearly about 100% although it does decrease slightly when all nodes in the network are stationary (pause time =500 s).

The average value of SRDLUP is equal to 0.973, and the maximum value is 0.99 which is at pause time 60 sec. this is because the location update packet just needs to be forwarded to nodes that are always closest to the centre, irrespective whether it is mobile or stationary.

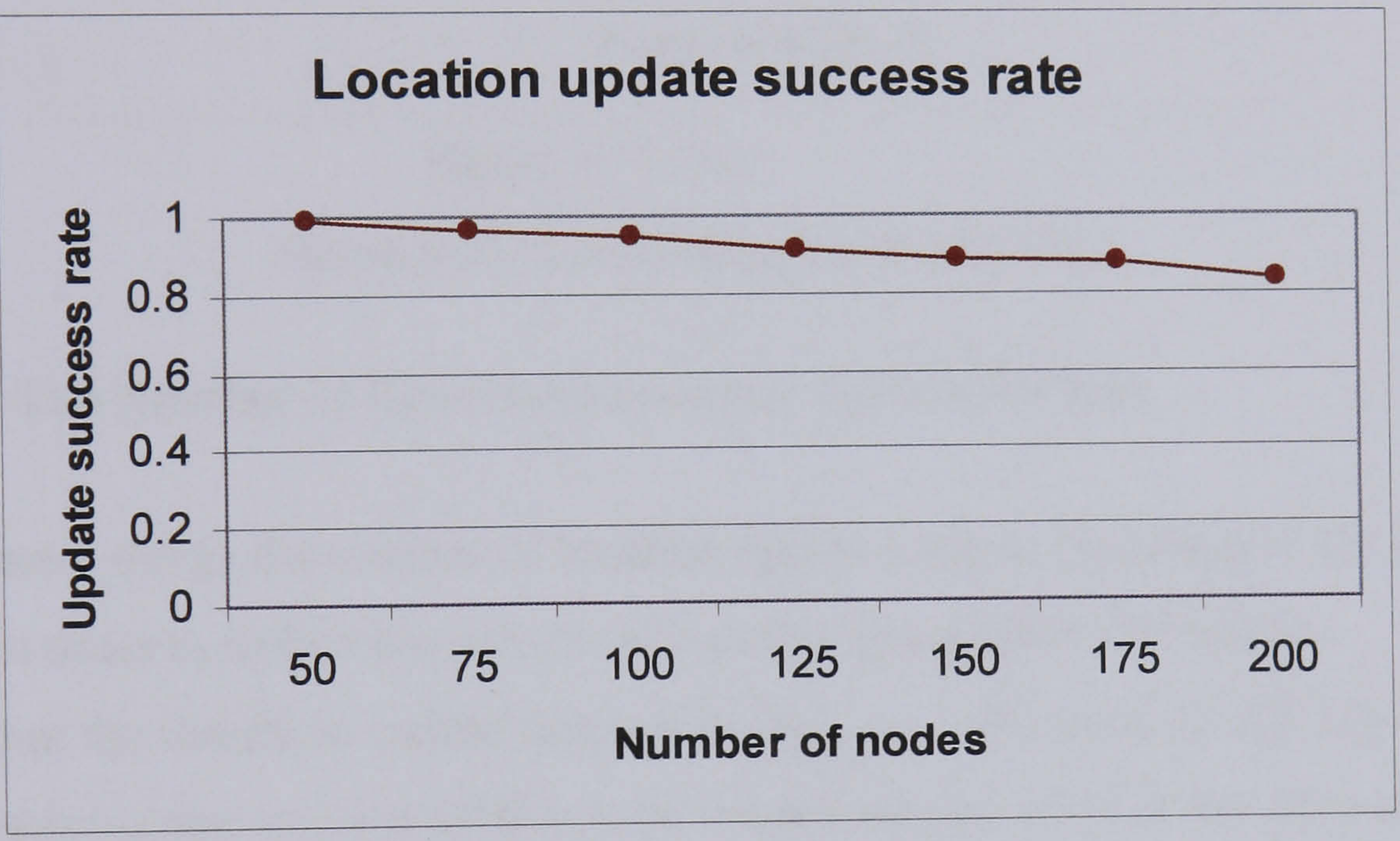


Figure 8-11: (a)

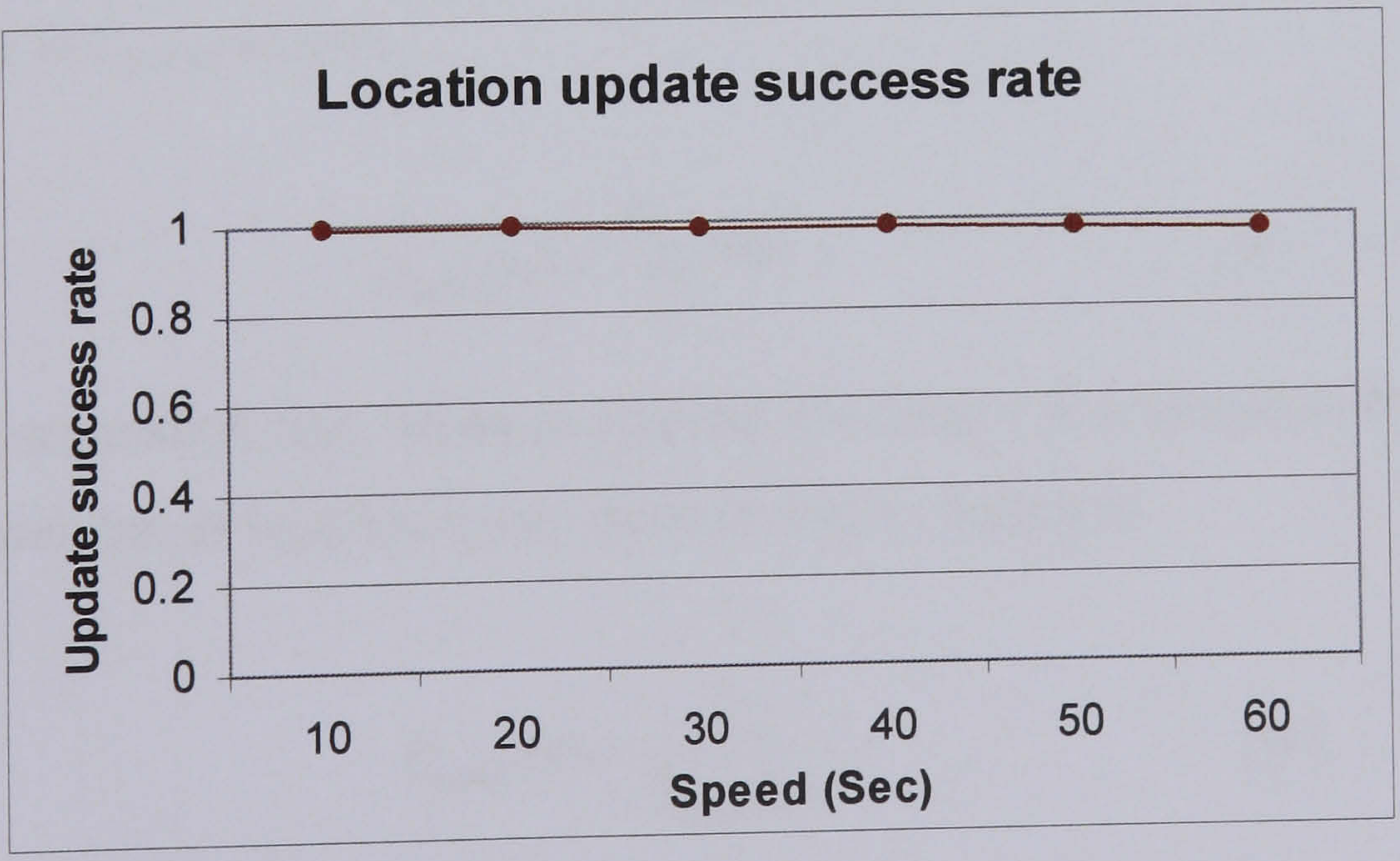


Figure 8-11: (b)

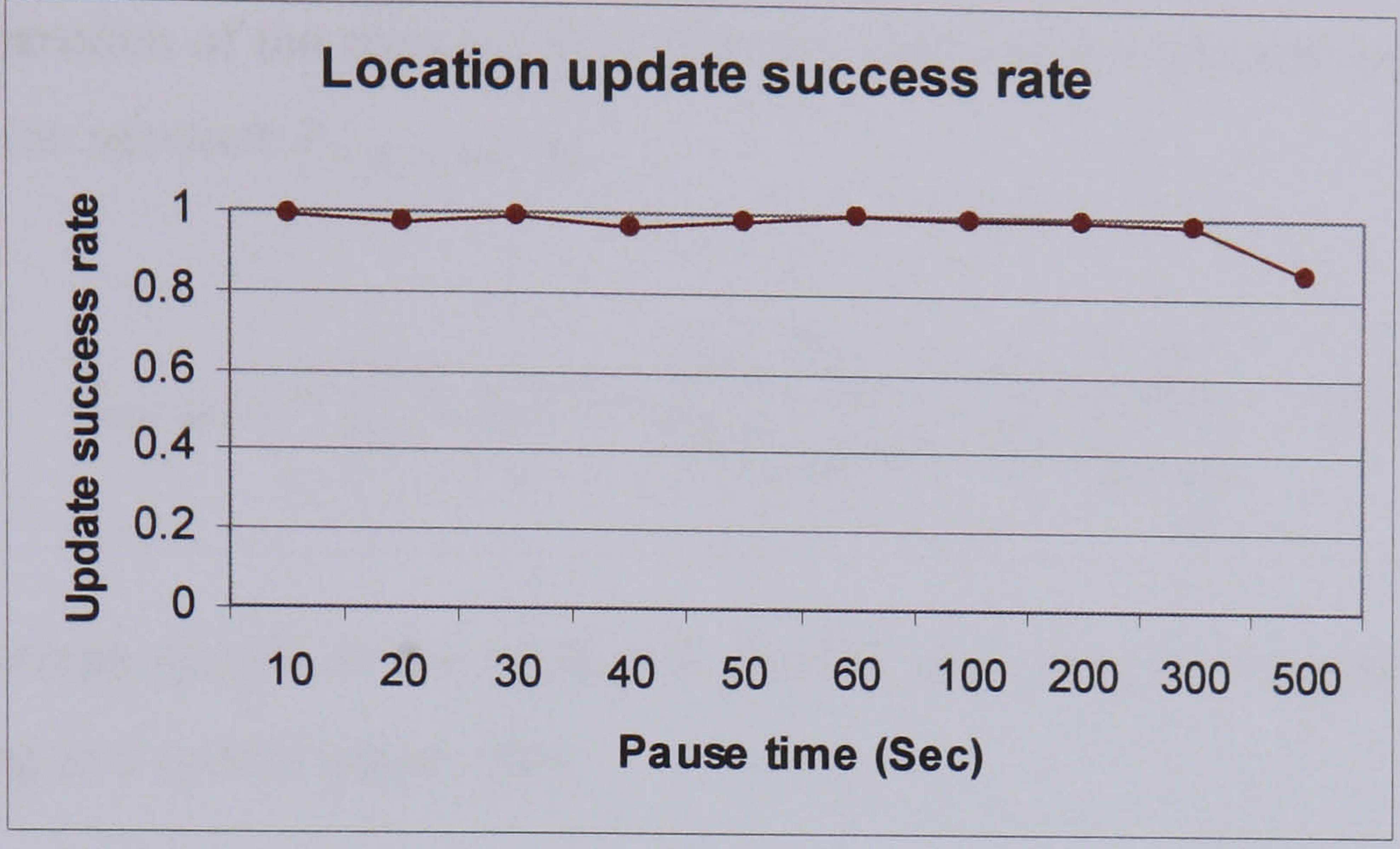


Figure 8-11: (c)

Figure 8-11: Location update success rate.

8.10.2.3 The Number of Generated Location Update Packets

This parameter shows the number of location update packets generated in the network by the nodes in order to update the servers with nodes' geographical locations.

Consider that the threshold update distance is $D_{threshold}$. The node should send an update packet containing the location of this node toward servers when it traverses $D_{threshold}$. If the average speed of a node, *n,* is V_n, and the time that the node *n* needs to trigger the update packet is $T_{update}(n)$ then:

$$T_{update}(n) = \frac{D_{threshold}}{V_n} \tag{9}$$

Consider the simulation time or the period that the node *n* is available in the network is T_{sim} then the number of location update packets sent by node *n* is:

$$P_{update}(n) = \frac{T_{sim}}{T_{update}(n)} \tag{10}$$

Consider the number of nodes available in the network during the simulation time or during the operation of the network is N then the total number of location update packets generated in the network P_{total_update} is:

$$P_{total\_update} = \sum_{n=1}^{N} P_{update}(n) = \sum_{n=1}^{N} \frac{T_{sim}}{T_{update}(n)} = \sum_{n=1}^{N} \frac{T_{sim} V_n}{D_{threshold}} \qquad (11)$$

When the average speeds of the nodes are simular and equal to V (such as in a tourists group walking in a certain place) then

$$P_{total\_update} = NP_{update} = \frac{NT_{sim}}{T_{update}} = \frac{NT_{sim} V}{D_{threshold}} \qquad (12)$$

By considering T_{sim} , $D_{thresold}$ and V are constants then

$$P_{total\_update} = K_{coeff} N$$

Where
$$K_{coeff} = \frac{T_{sim} V}{D_{threshold}} \qquad (13)$$

For example, if the T_{sim} = 500 sec, $D_{threshold}$ = 25, and V = 5 then the P_{total_update} calculated theoretically by the previous equation and the simulation result for different number of nodes are shown in Figure 8-12. From Figure 8-12, it can be seen that the number of update packets generated by the simulation is less than that generated theoretically because the nodes do not exactly have the same speed. Figure 8-13 shows the the number of generated location update packets against the number of nodes, speed, and mobility (pause time). As can be seen the generated packets are

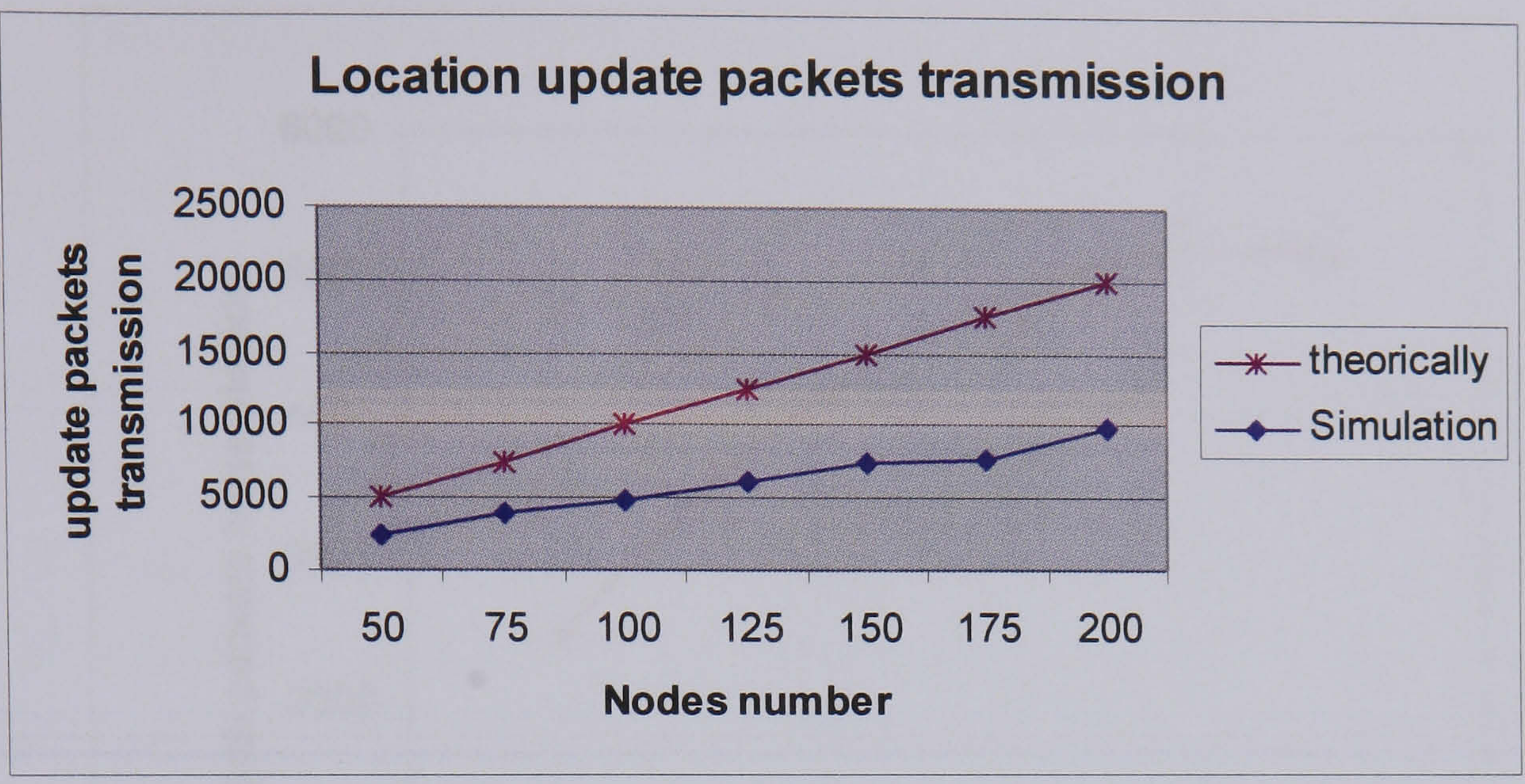


Figure 8-12: The number of generated location update packets

increasing gradualy with increasing the number of nodes and speed while decreasing gradually with increasing the pause time (toward more stationary) until it reaches to nearly zero at pause time 500 where all nodes are stationary and no longer need to generate update packets.

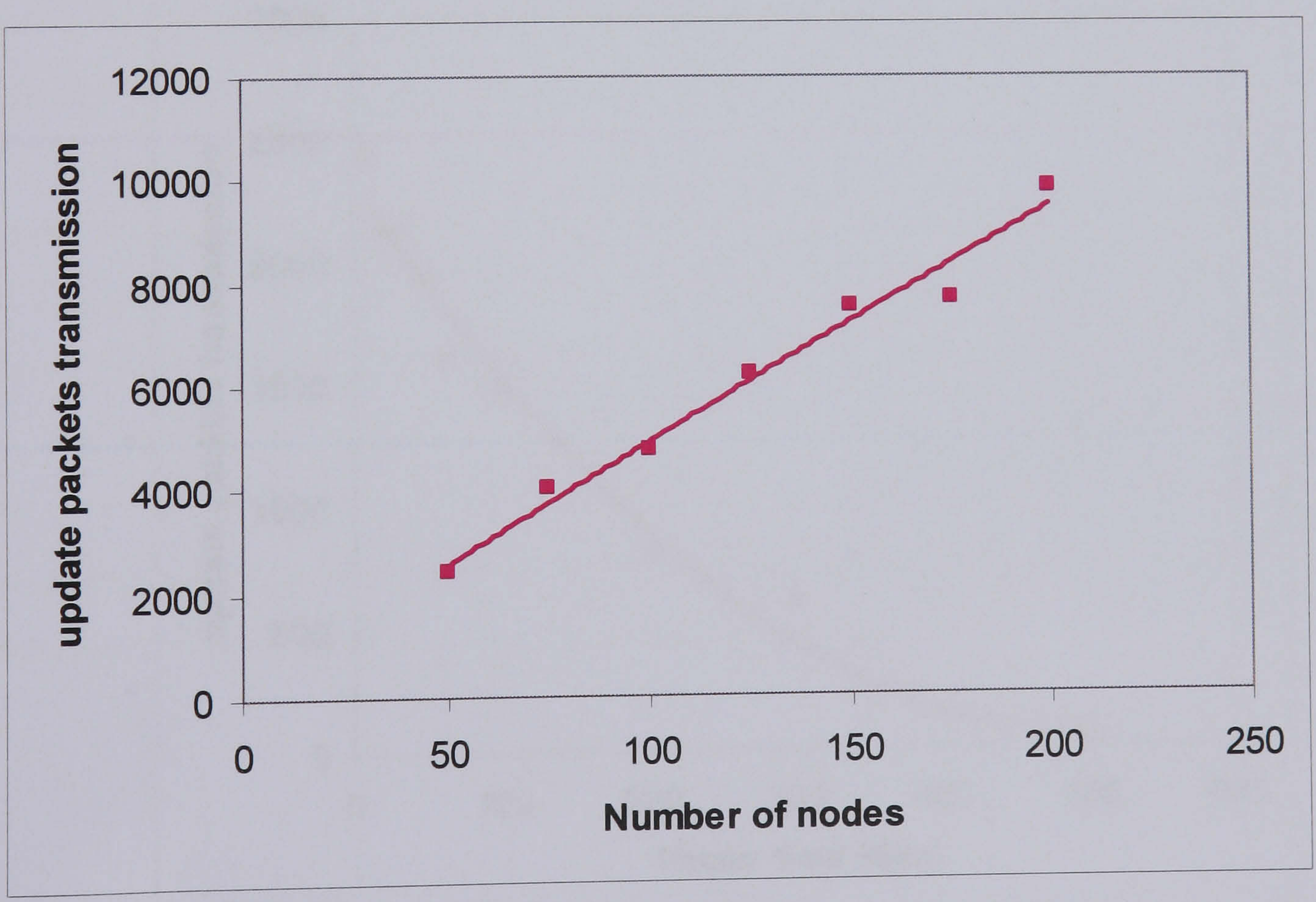


Figure 8-13: (a)

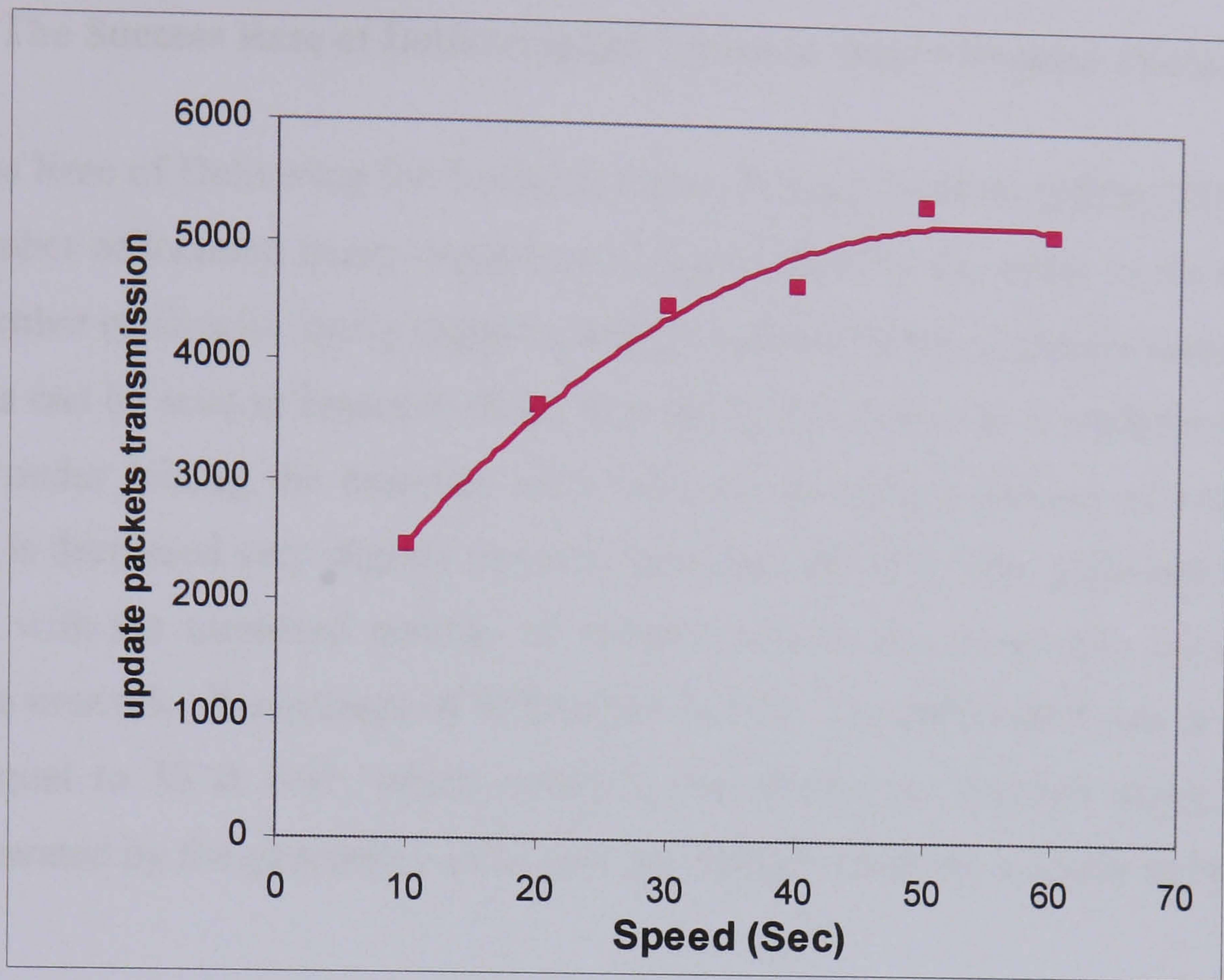


Figure 8-13: (b)

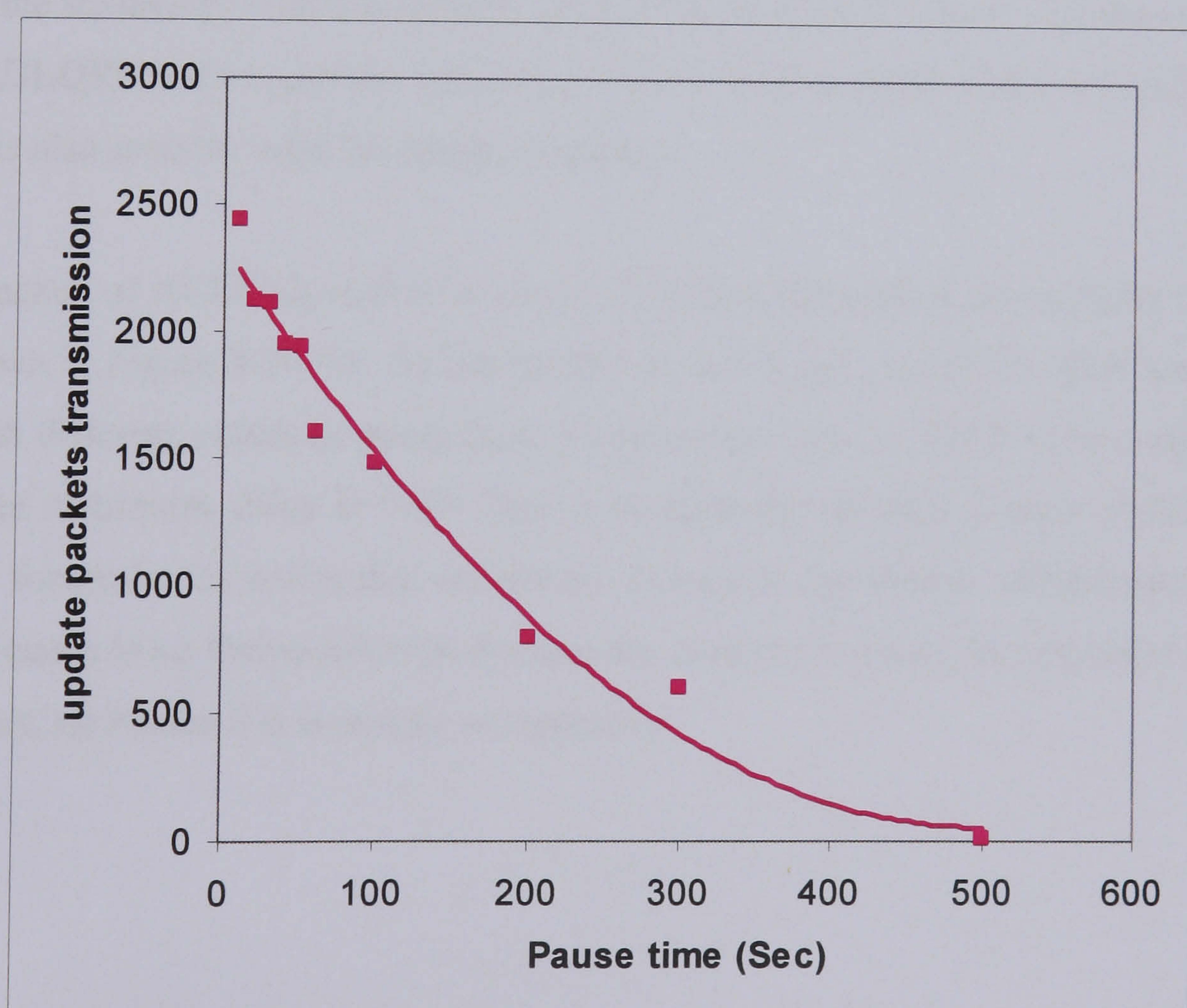


Figure 8-13: (c)

Figure 8-13: the Number of generated location update packets

8.10.2.4 The Success Rate of Delivering the Location Query Request Packets

The Success Rate of Delivering the Location Query Request Packets (SRDLQRP) is the ratio of number of location query request packets generated by the nodes in the network over the number of location query request packets received by the originator nodes of the requests. As can be seen in Figure 8-14 (a) that the ACLS algorithm is scalable with the number of nodes joining the network, since with the increasing number of nodes, the SRDLQRP is decreased very slightly and remains above the 87%. The slight reduction in SRDLQRP with the increased number of nodes is due to the congestion incurred by nodes in the network. The average of SRDLQRP is 0.89. The SRDLQRP rate at number of nodes equal to 50 is 0.97, which indicates that almost all location query request packets generated by the generator nodes have got replies about the location of requested nodes.

In terms of the scalability with the speed of nodes, Figure 8-14 (c) shows that the average value of SRDLQRP is 0.95, and the maximum value is 0.97 at speed 10m/s. this indicates that ACLS is also scalable with the speed of nodes.

The performance of ACLS algorithm in terms of SRDLQRP against the mobility (pause time) is shown in Figure 8-14 (b). As can be seen in this figure, the SRDLQRP is almost constant with different values of pause time. The average value of SRDLQRP is equal to 0.97, and the maximum value is 0.99. This is because the location request packet just needs to be forwarded to nodes that are always closest to the centre, and request reply packets just needs to be forwarded to nodes that are always closest to the originator of the request packet, no matter if it is mobile or stationary.

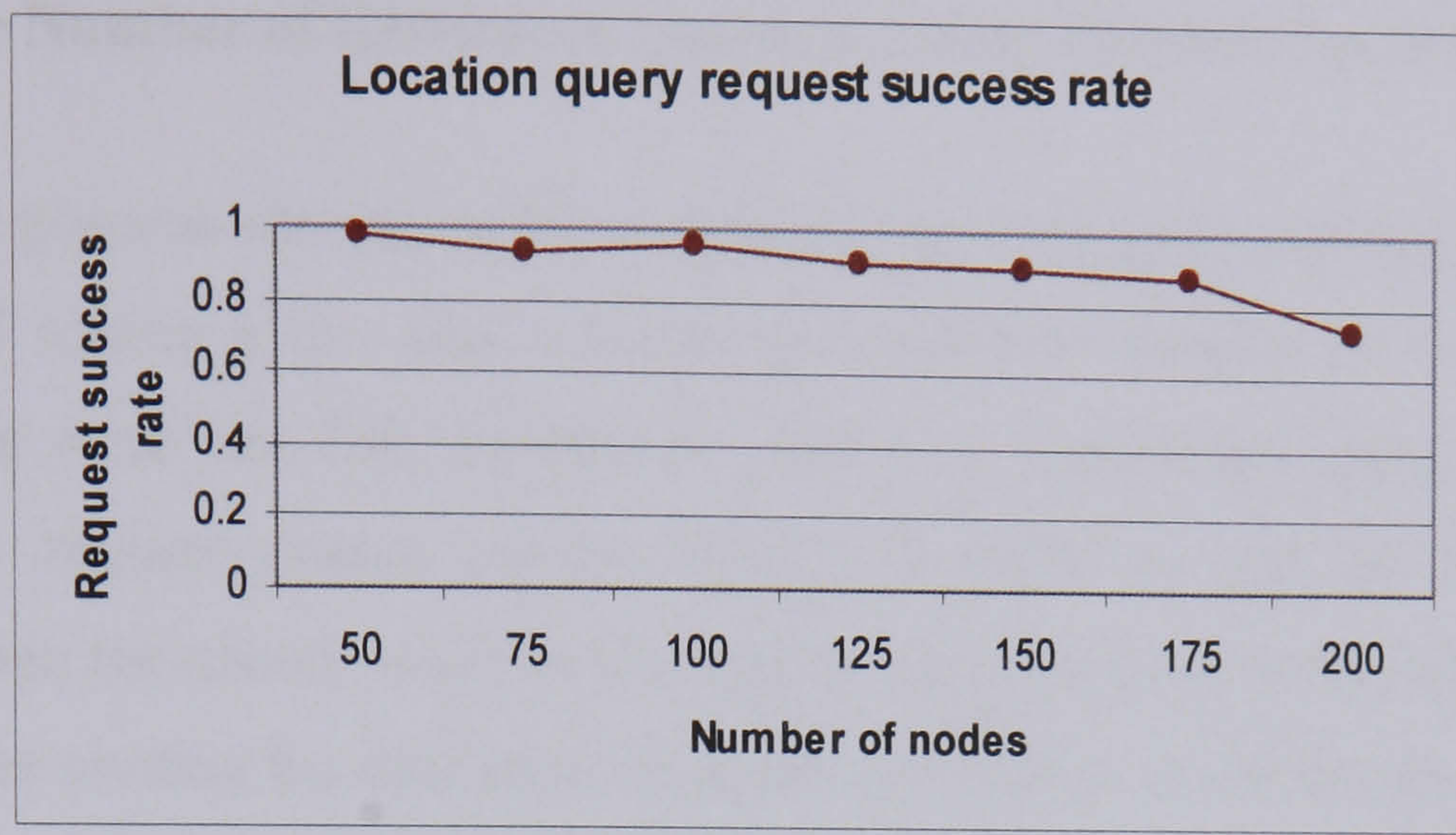


Figure 8-14: (a)

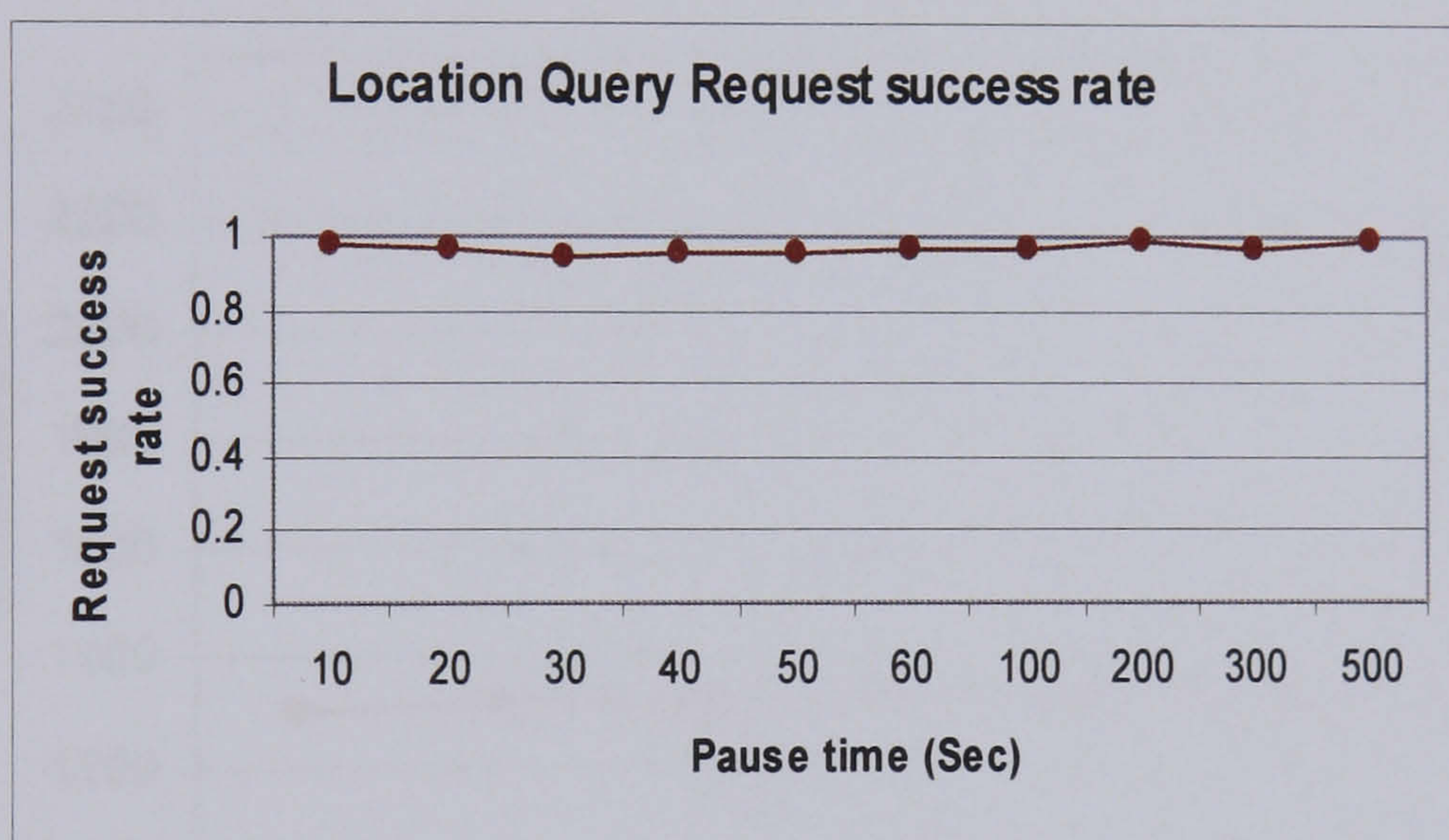


Figure 8-14: (b)

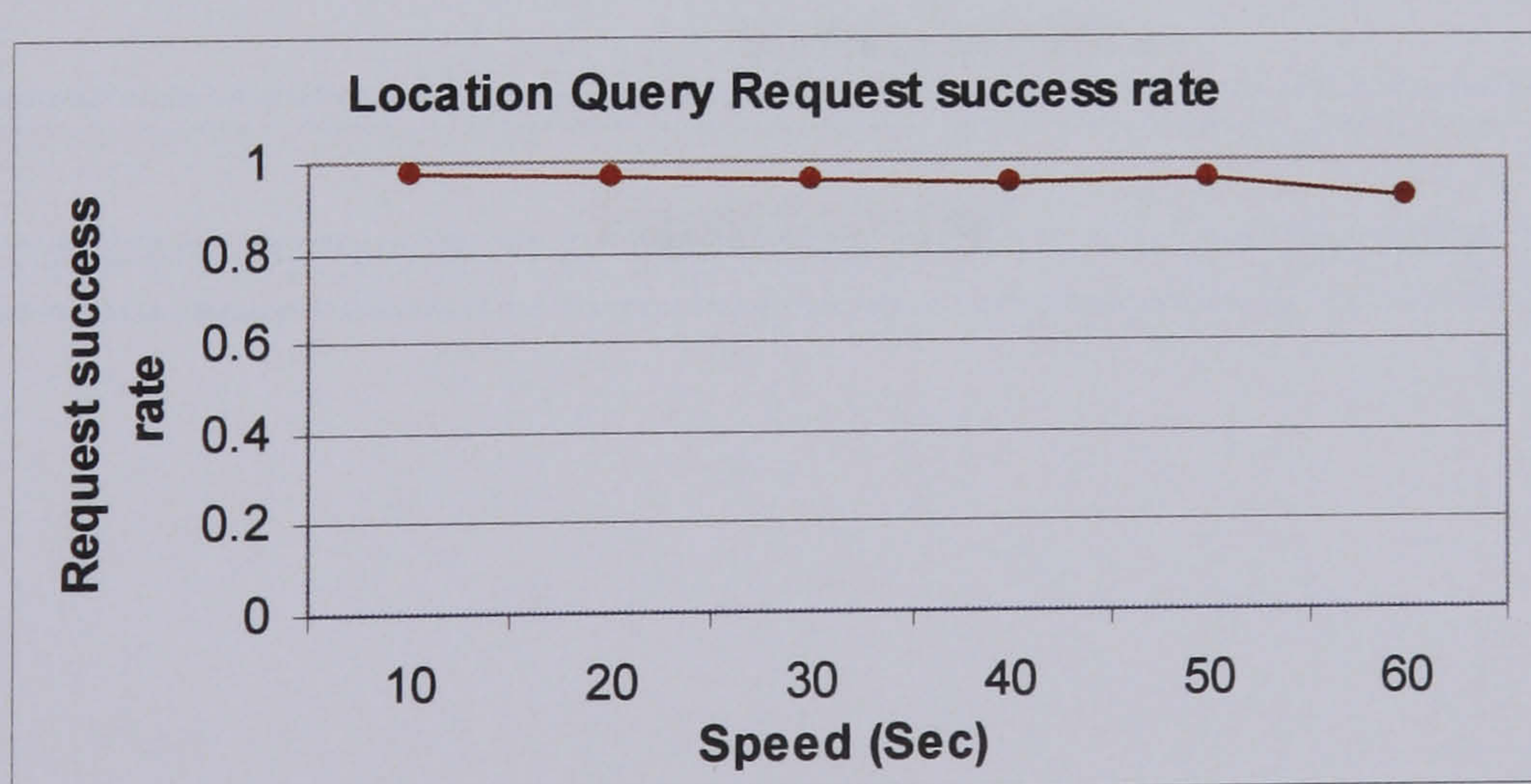


Figure 8-14: (c)

Figure 8-14: The success rate of delivering the location query request packets

8.10.2.5 The Number of Generated Location Query Request Packets

This parameter gives an idea about the number of location query requests generated in the network by all source nodes that required geographical location of their destinations. When a source node has data packets to send to a destination node, it first sends a location query request packet toward servers in order to get the location of that destination, when the source receives the request reply packet that includes that location, the source starts sending the data packets to the destination. It can be seen in Figure 8-15 that the number of location query request packets is nearly constant and scalable with the number of nodes , speed and mobility (pause time).

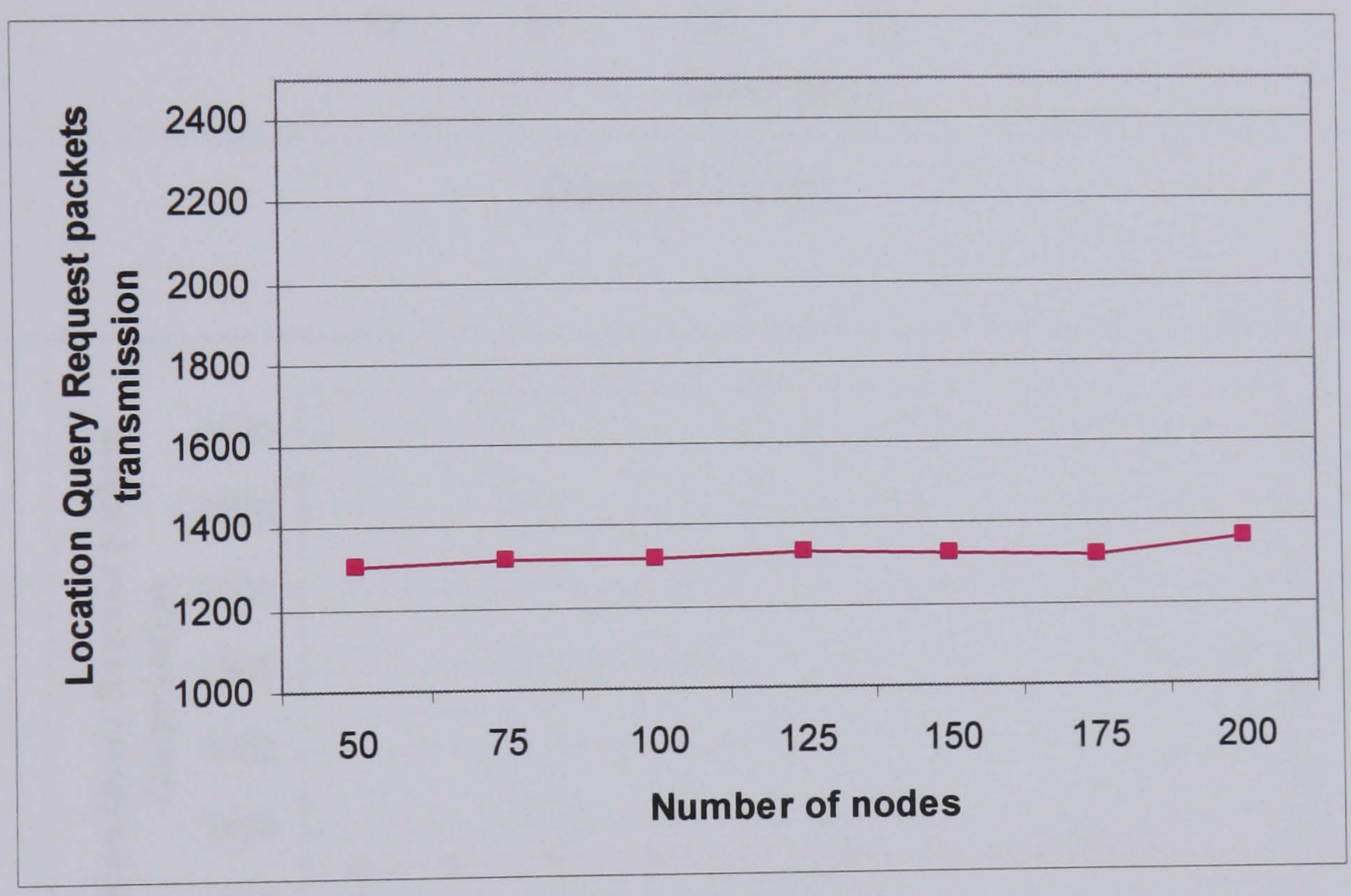


Figure 8 15: (a)

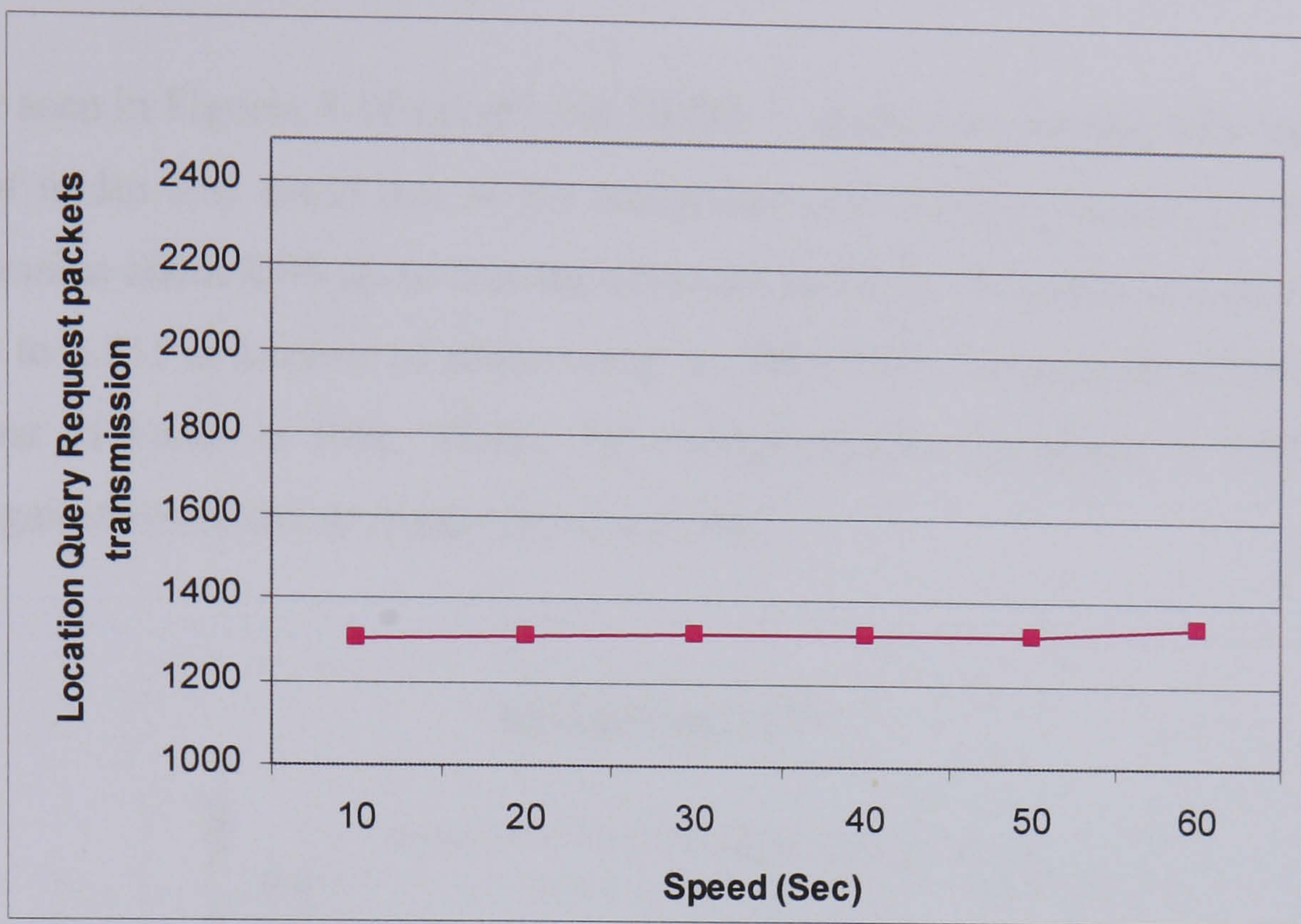


Figure 8-15: (b)

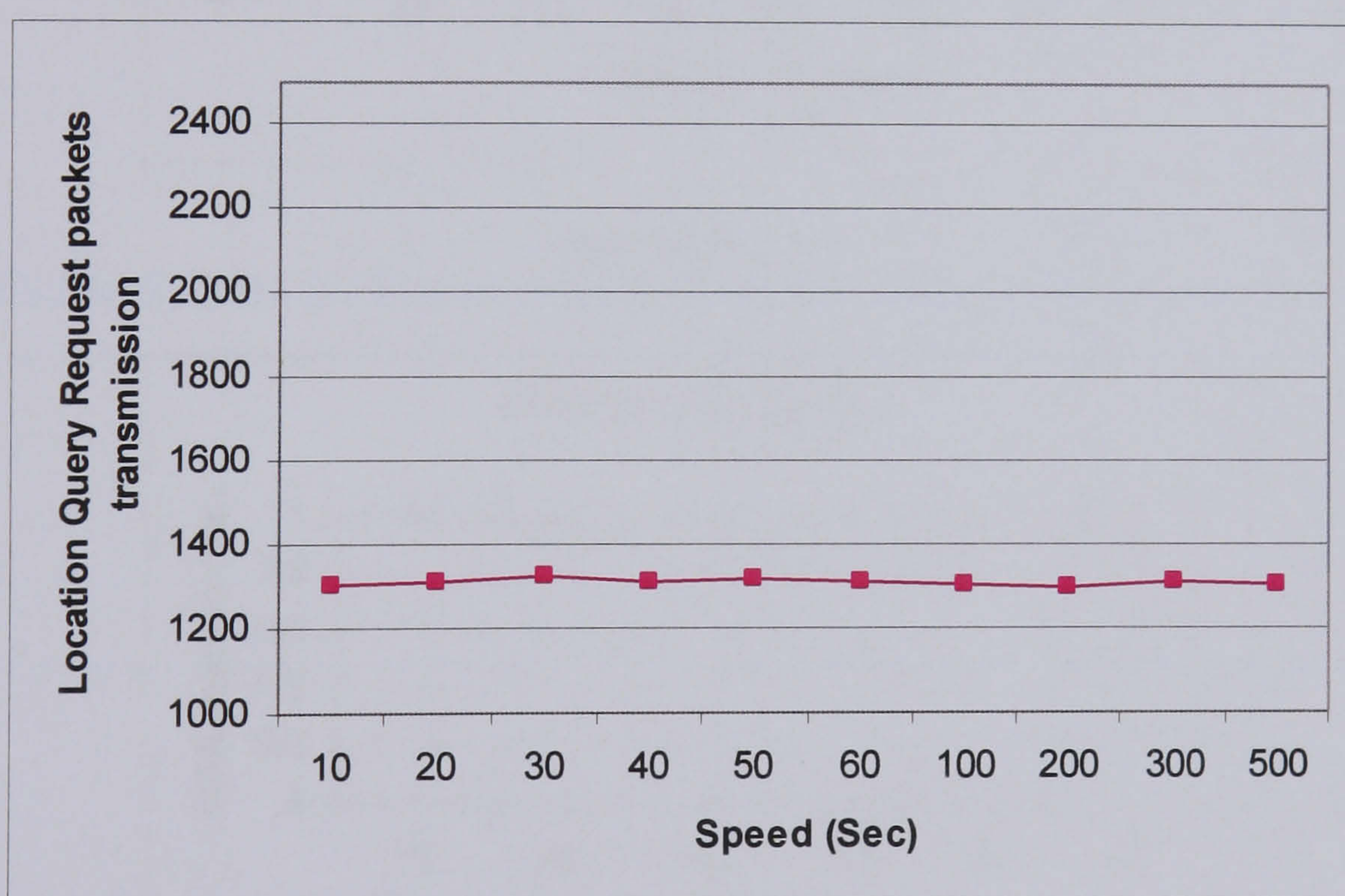


Figure 8-15: (c)

Figure 8-15: The location Query Request packets transmission

8.10.2.6 The Data Packet Delivery Ratio

The Data Packet Delivery Ratio (DPDR) is the number of data packets that are received by the intended destinations over the number of data packets sent by the source nodes.

As can be seen in Figures 8-16 (a) (b) that DPDR is slightly decreasing with increased the number of nodes and speed due to the congestion and mobility caused by nodes. The DPDR remains about 0.95 up to number of nodes equal to 150 nodes and decreases after that to up to 0.815 at number of nodes equal to 200 nodes. The average of DPDR against the number of nodes is 94%. Whilst the average against the speed is 0.973, and the average against the mobility (pause time) is 0.986.

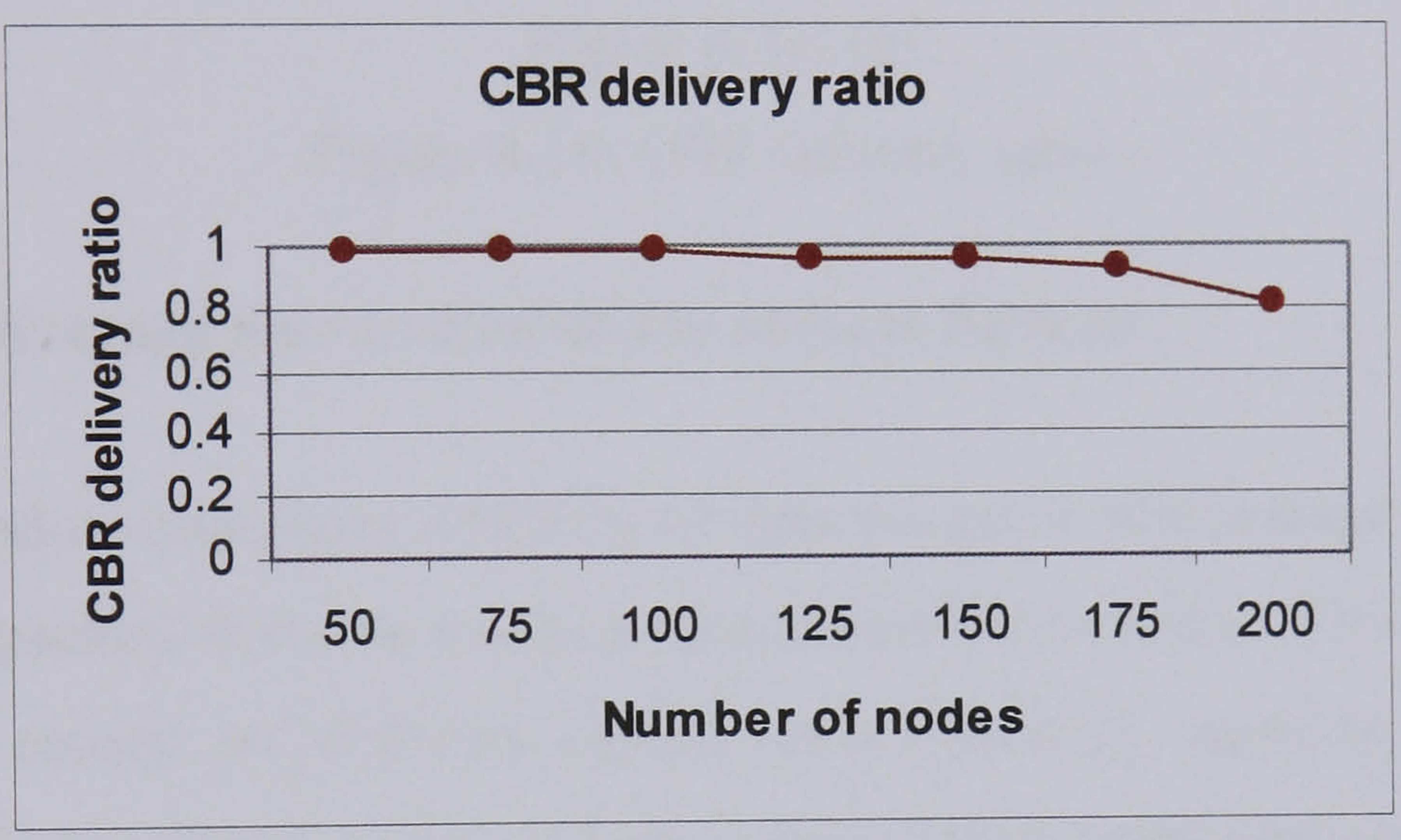


Figure 8-16: (a)

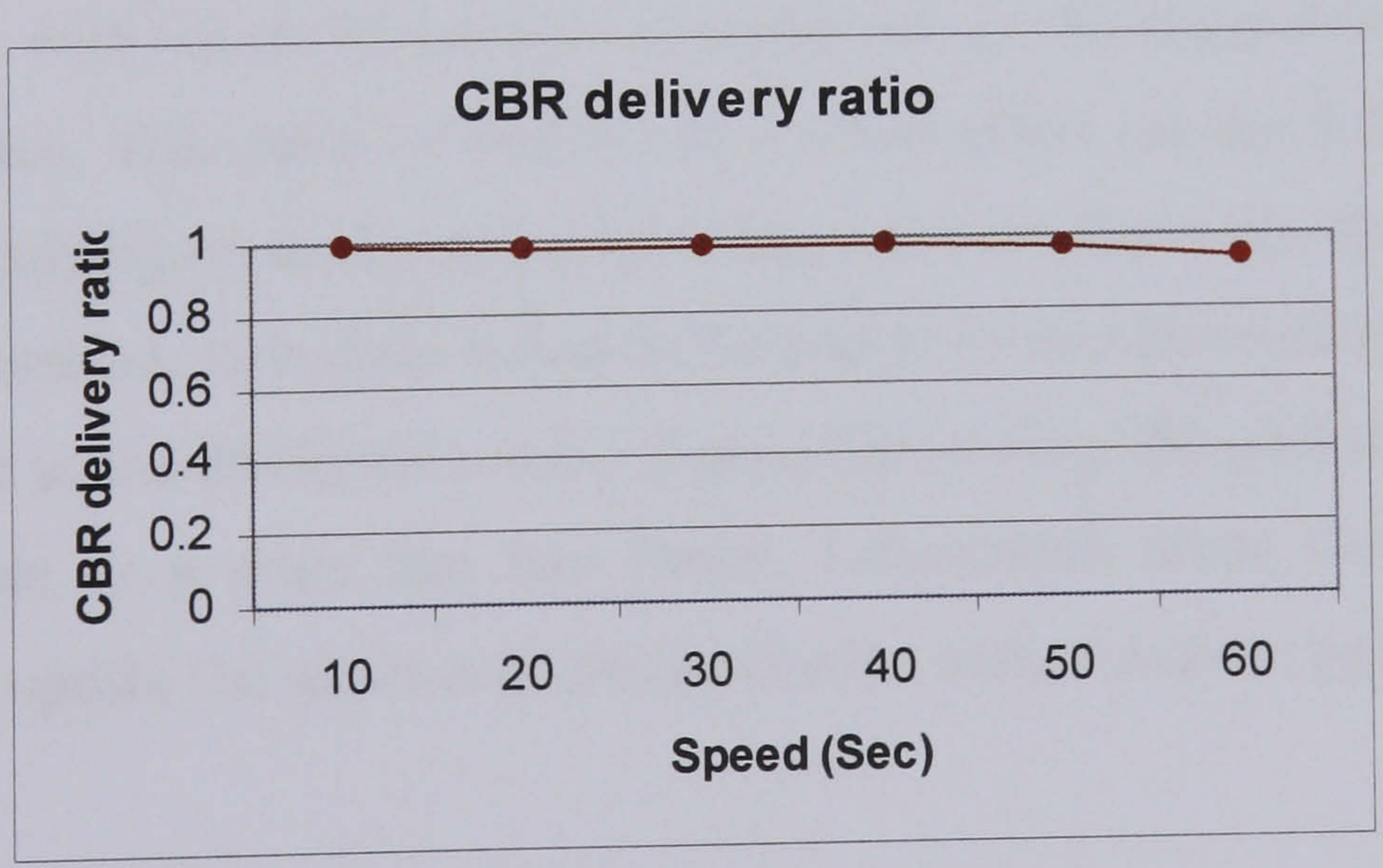


Figure 8-16: (b)

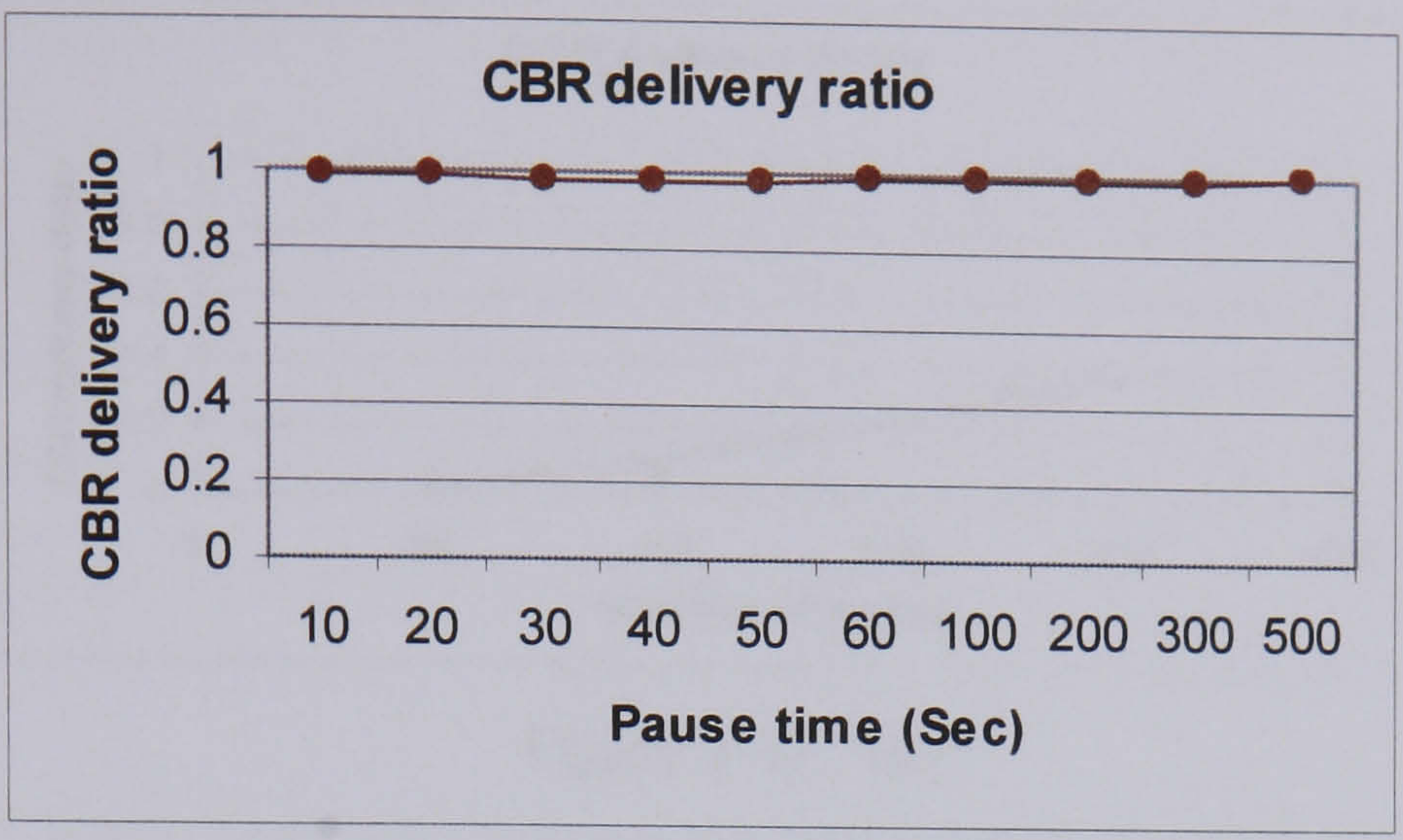


Figure 8-16: (c)

Figure 8-16: CBR delivery ratio

8.10.2.7 The Average End-to-End-Delay of Data Packets

The Average End-to-End-Delay (AEED) of data packet is the average time required to deliver the data packets from the source nodes to destination nodes. This time includes all possible delays caused by buffering during route discovery, queuing at the interface-queue, retransmission delays at the medium access control layer, propagation and transfer times and ARP delay that has a considerable value. It can be seen in Figure 8-17 (a) that AEED increases with increased number of nodes due to the congestion and contention occurred by nodes. The speed of nodes has a small effect on the AEED because the packets are not relying on an already established and complete route from the source to the destination. Instead, each node forwards the packet to next downstream node that is as close as possible to the destination node. During forwarding, the packet, if it is received by a server node or a node that has fresher information about the location of the destination, will update the location of the destination included in the packet itself.

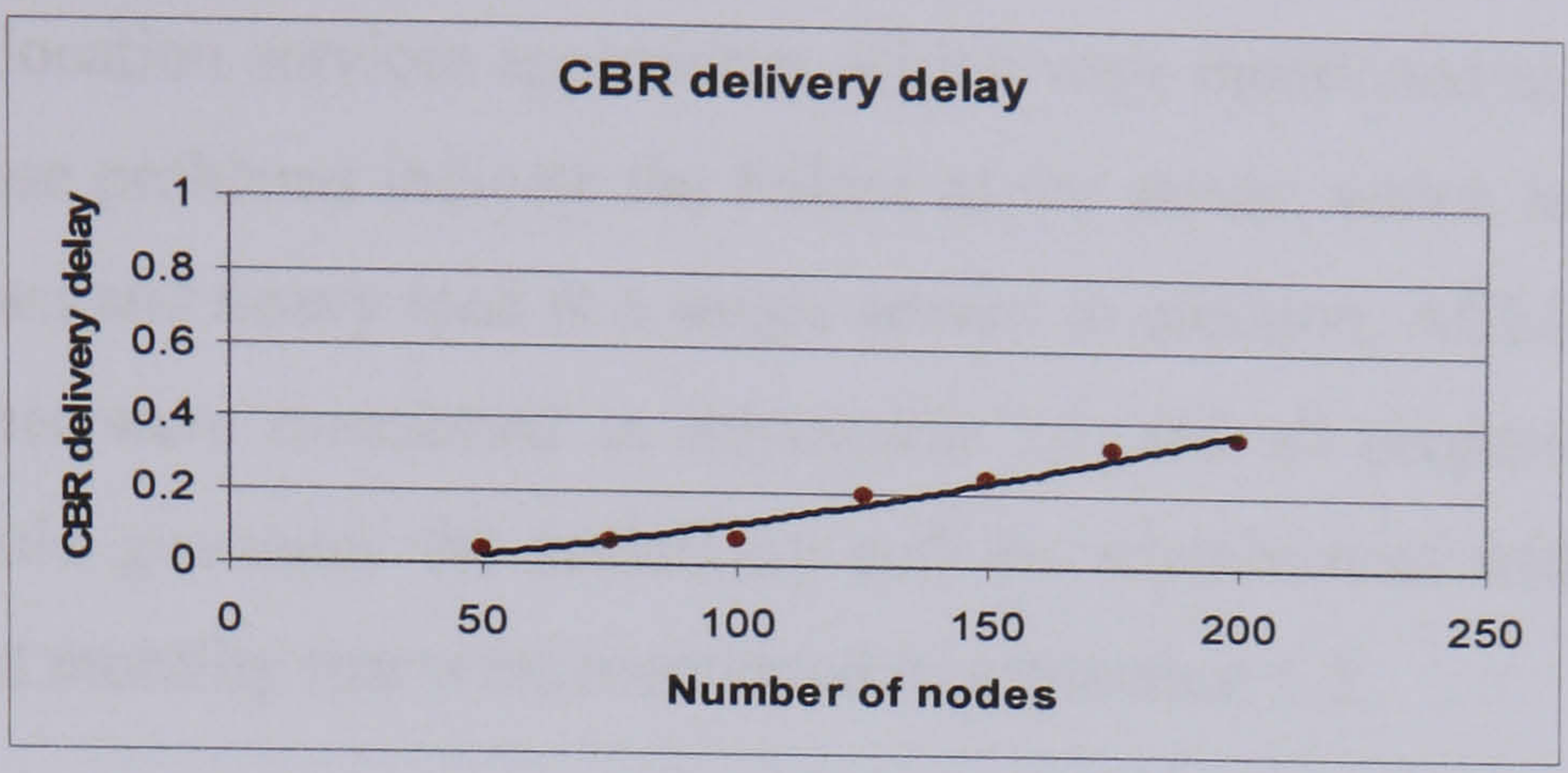


Figure 8-17: (a)

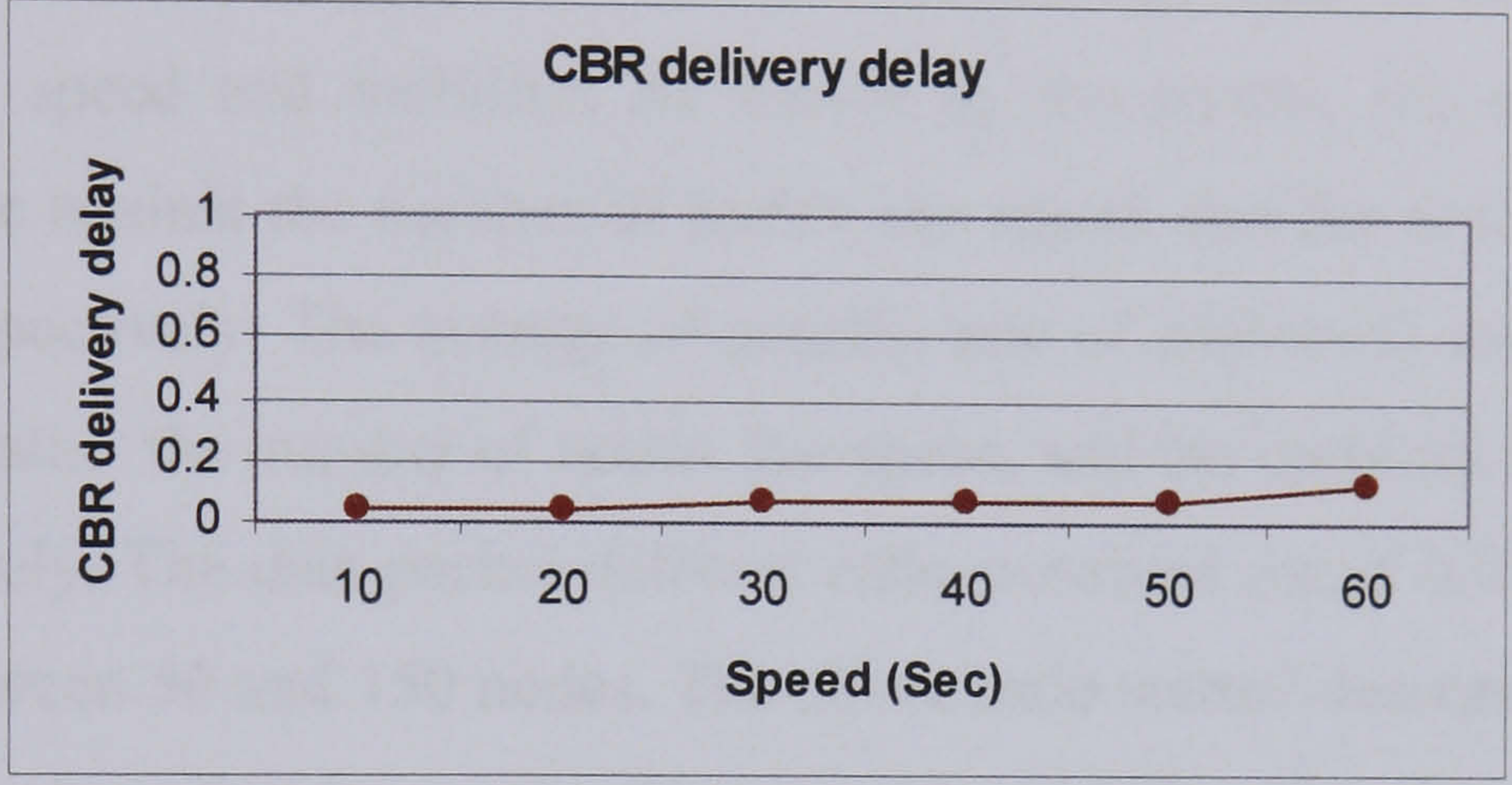


Figure 8-17: (b)

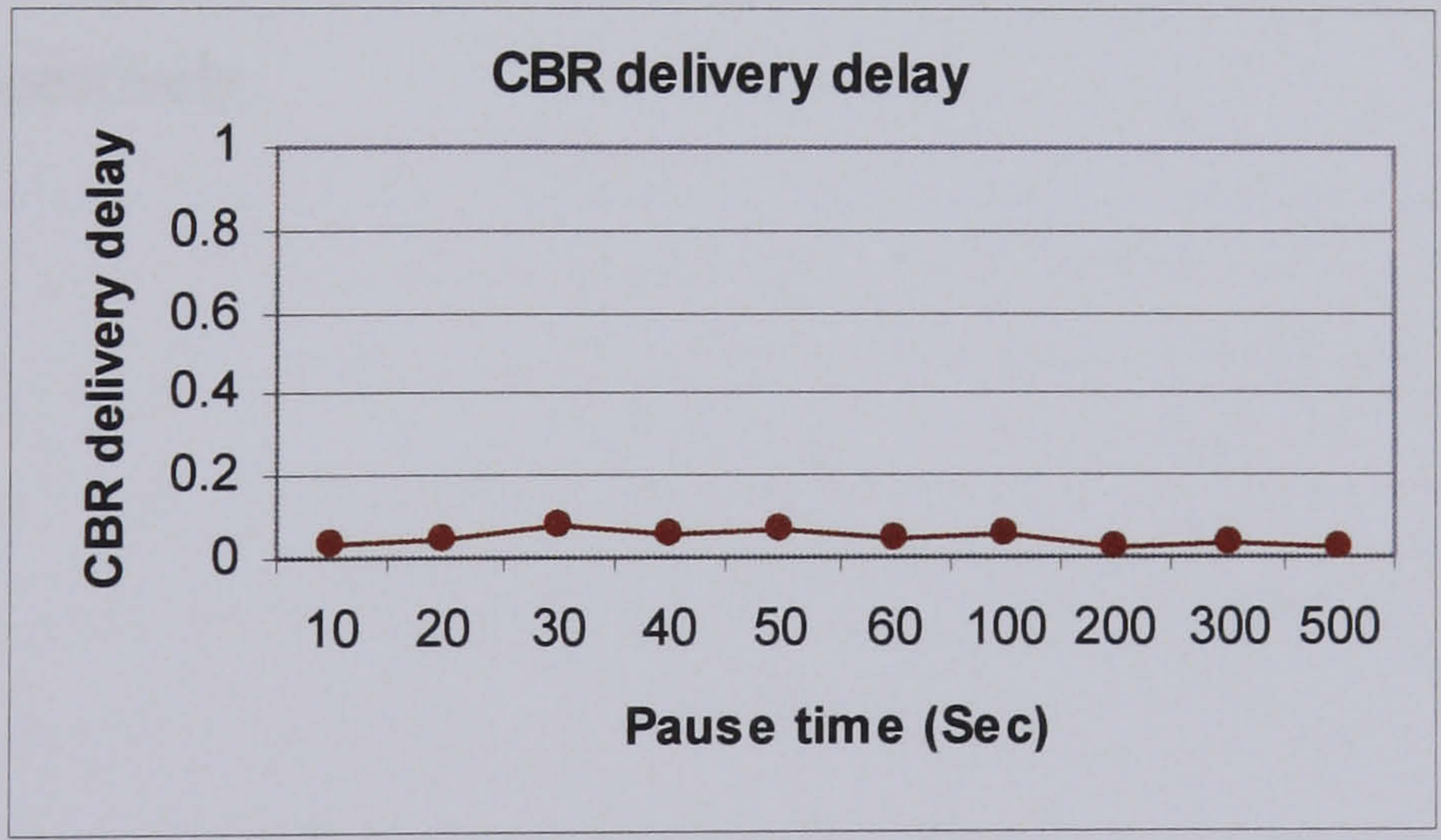


Figure 8-17: (c)

Figure 8-17: End-to-end-delay of data packets

8.11 Summary

In this chapter, a new Adaptive Centralised Location Service (ACLS) was presented. ACLS tracks mobile node locations. ACLS overcomes the main problems of centralised static servers in location services approaches, which were mentioned in the beginning of this chapter. These problems indicate the failure of the server, which leads to the whole system to go down and heavy load at a single server. In addition, ACLS also has met all the objectives that were mentioned in subsection 1.2, and all properties of a location service that should guarantee the scalability and the adaptiveness with the number of nodes, speed, and mobility that were mentioned in subsection 1.3.

Results have shown that the proposed location service approach is scalable with the number of nodes, speed and mobility. As shown by the results, the average location update success rate against the number of nodes, the speed, and the mobility were 0.92, 0.98, and 0.97 respectively. The average of success rate of delivering the location query request packets against the number of nodes, the speed, and the mobility were 0.89, 0.95, and 0.97 respectively. The data packet delivery ratio remained round 0.95 for number of nodes ranging between 50 and 150 nodes. The above ratio started decreasing after that to reach 0.815 for number of nodes ranging between 50 and 200 nodes. The average of data packet delivery ratio against the number of nodes, the speed, and the mobility were 0.94, 0.97, and 0.986 respectively.

Chapter 9

Case Study and Applications

Mobile ad hoc networks are considered to be the future of wireless networks due to their specific characteristics (practical, simple, self-organization, self-configuration, easy to use and inexpensive as operating in a license free frequency band).

There are many applications to ad hoc networks, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic mobility such as:

- In education, ad hoc networks may be deployed for student laptops interacting with the lecturer during classes.
- Inter-Vehicle Communications, ad hoc networks for vehicles, for example, sending instant traffic reports and other information between drivers.
- Electronic email and file transfer,
- Web services that can be used by ad hoc network users in case a node in the network serves as a gateway to the outside world.
- A wide range of military applications, such as a battlefield in unknown territory where an infrastructure network is not available or impossible to maintain.
- Collaborative work for business environments.
- Emergency search-and-rescue operations, in disaster areas where it is almost impossible to implement an infrastructure network.
- Personal Area Networking (PAN) and Bluetooth.
- Electronic payments from anywhere (i.e. taxi).
- Home Wireless Network.
- Office Wireless Network.

During the period of this research, a framework is proposed for an important application of mobile ad hoc networks [23]. This framework is for implementing and using mobile ad hoc networks in the telecare system in order to help elderly people to get better treatments. Next section elaborates the framework.

9.1 Telecare Proposed System

The needs of telecare system have to be specified as well as defining the problem to be treated. Then, a framework has to be designed for this telecare system.

9.1.1 Problem definition

Designing and developing a self-configurable framework based on new technology solutions are aimed at stopping or minimising the institutionalisation of elderly citizens. This framework has been, for sometime now, a fundamental challenge for Research and Development (R&D), healthcare and welfare systems and services, governments, and the private sector. This is fundamental with the mounting cost in healthcare and increased pressure burden on maintenance, caring and sustaining of nursing homes. When deployed, such solutions will allow the elderly to safely and happily remain in their own homes, and maintain the administration, management, and monitoring of elderly and less-able individuals to a high level of satisfaction. An effective and affordable system will utilise the integration of interoperable, autonomous, self-configurable, intelligent, wireless mobile agents and an allied information management approach, combined with the services applied to assist the user. Therefore, the envisaged objectives of "UK Telecare Solution" project are to improve the quality of life and care for the elderly, deliver care in real-time, act as an early diagnostics and intervention system, and increase the number of consultations for elderly people and their families.

9.1.2 Requirement

The framework requires combination of live audio, a two-way video connection and monitoring technology equipped with a variety of medical peripherals, all aimed to create a flexible, and user-friendly patient-specific home Telecare systems. The self-contained unit, which is usually installed in a patient's home (patient station), enables the patients to personally carry out tests or taking measurements for so many parameters related to the disease or to the body condition (e.g., blood pressure, temperature, electro cardio graphic, etc.). This information then needs to be transmitted digitally over the air interface using a wireless multimedia device to the specialised health centres to remotely interact from a variety of locations.

The patient station should be able to establish connection through any network access point in the patient's home. In this regard, a wireless network is fundamental in assisting patients to send peripheral equipment's reading from any location at home.

9.1.3 The Built Environment

Cost and ease of installation is an issue for home network systems in general. While it is relatively easy to design a new home or apartment block to accommodate the necessary network infrastructure with the current infrastructure, most people live in homes where such facilities are not available. Hence, a market strategy that depends on traditional networks installation in new-build properties only is likely to fail. Therefore, this proposal is based on employing the MANET and wireless sensor networks for augmenting the home care services provided to the elderly people. This would involve considering the patients that need treatment at home to form an ad hoc network, in this way transmission of information will occur based on the patients demand. This process is relatively cheap as no infrastructure is required, it will not add to the (already congested) traffic of the normal communication system, and most importantly, it fits the nature of the problem considering the patient distribution in the large cities.

Using a "wireless sensor network" technology approach provides distributed network access to sensors, actuators and processors embedded in a variety of equipment. These networks represent a new monitor and control capability for applications such as Telecare.

Existing routing protocols currently used in mobile ad hoc network should support services such as Multimedia services (voice, video and data), and should guarantee acceptable QoS, in terms of information security to keep the patient's information secure, adaptation to mobility, and reliability (the information should be guaranteed to be received). Securing patient's information includes protection from any kind of interference such as eavesdropping, tampering, and impersonation by using a set of well-established techniques known as public-key cryptography, which facilitate encryption, and decryption of the patient's data, tamper detection, authentication, and nonrepudiation.

An essential operational issue in the system will assume that the patient will hold his/her ad hoc mobile device all the time. The device maintains and frequently updates a database of information regarding the patient's illness by logging it to the patient station and downloads the information records. In occasions when the patient is outside the home network, he/she could press the emergency button on the device. The device will then scan the local area, searching for other devices to connect to thus, allowing the patient to communicate with the nearest mobile ad hoc device or cellular device or access point nearest to him/her to guarantee the communication with the health centre, and download the information saved on his/her device to that device to call the nearest emergency unit for timely and speedy intervention.

The nodes or sensors will be distributed in different locations in the home and the patient will hold his/her mobile device all the time; this device:

a) Maintains and frequently updates a database on information of patient's illness.
b) Capable of downloading the information from the patient station.
c) Has an emergency button on the device to search and connect to the other devices in emergency situation.

The patient station used for measuring the many condition parameters is a wireless device to transmit this information over the air (should be able to establish connection through network device (access point, sensor, ad hoc device).

The routing protocol that is implemented in all ad hoc devices and sensors should provide the following requirements:

1. Support multimedia services (audio, video).

2. Support acceptable QoS for some parameters.
3. Support low level of security.
4. Support reliability (patient's information should be guarantied to be received)
5. Capable to connect to access point that is connected to landline phone.
6. Capable to connect to nearest cellular device
7. Capable to searching for: first ad hoc device(mobile or sensor), if the device not found it will start looking for access point, if access point not found it will start searching for nearest cellular device.

Using the third protocol proposed in this thesis (HARP3) is suggested. This protocol should support the requirements mention above. The perspective of the framework of the network is shown in the following Figure 9-1.

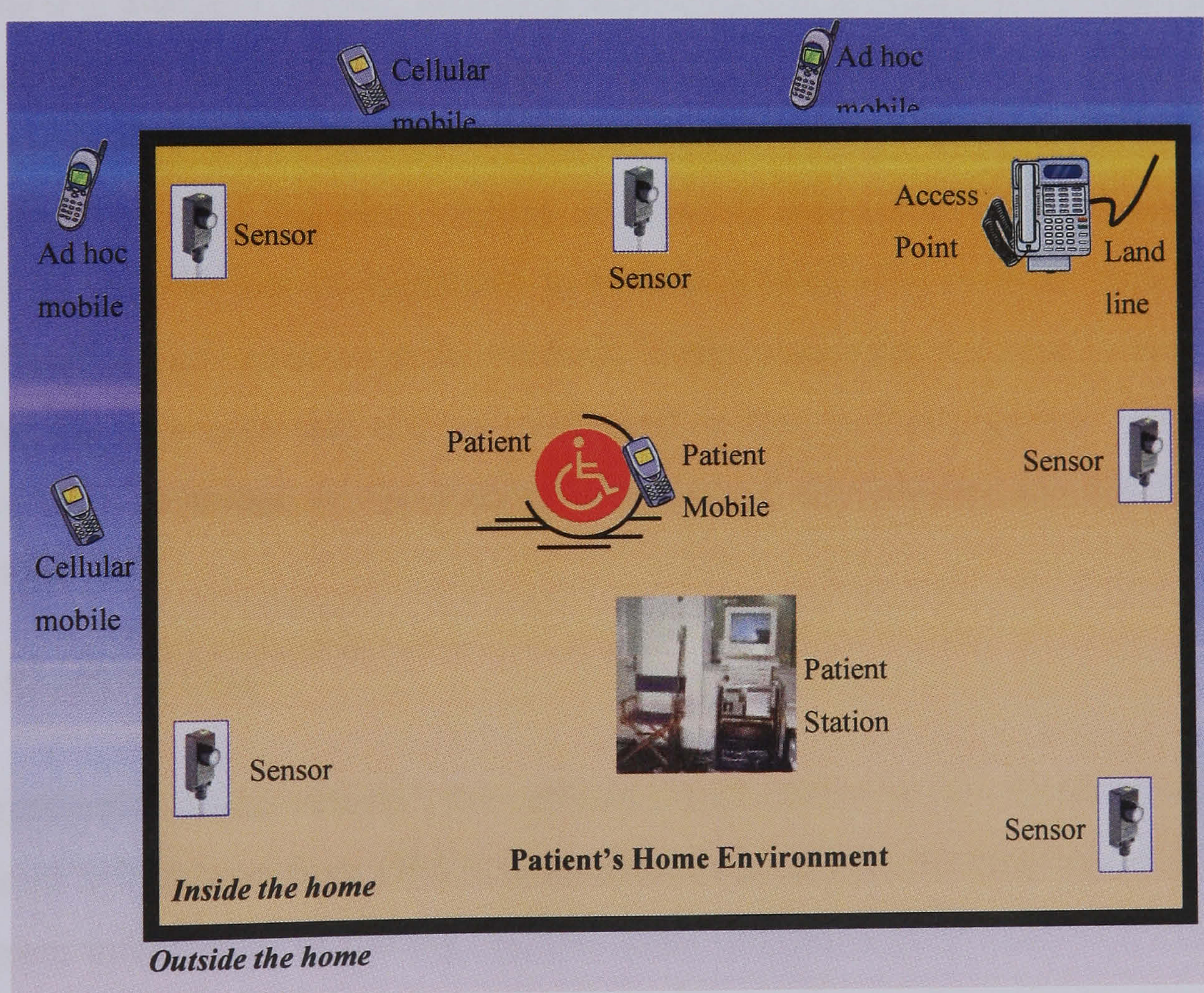


Figure 9-1: Framework for a telecare system

9.2 Inter-Vehicles Ad hoc System

Many applications of ad hoc networks have been developed in Inter-Vehicle communication. For example, exchanging safety and warning information between vehicles or between roadside sensors and vehicles travelling on the road. These applications have become an important research area for Intelligent Transportation Systems (ITS) telematics applications. The exchanged information will extend the perception horizon of the drivers. The goal here is to implement the proposed routing protocols for inter-vehicle communications based on mobile ad hoc networks.

As mentioned in chapter six, in some situations, the source of information used by the network is not available (such as GPS information in the underground) while in other situations it is available. Hence, protocols relying on this information will fail to perform their functions. In such situation, alternative self-content information should be available to the vehicle's devices to perform the needed task of routing. In this suggested system, an implementation of the three routing schemes is proposed. These schemes exploit mobility of vehicles and its directions to provide a long-lived route to destination and reduce flooding and overhead in the network. In these schemes, we appropriately remove receiving the messages that are not addressed to the received vehicle. The proposed schemes take advantage of the heading direction of the vehicles for establishing the packet route.

9.2.1 Scenario One

In the application "inter-vehicle", the vehicles usually move at very similar speeds and in some times information from GPS is unavailable (e.g., tunnels/undergrounds). Moreover, using more information in routing requires more resources to provide this information. These resources are most likely to be unavailable all together, and if one of these resources is absent, then the task of routing will fail. Therefore, only the most important "self-content" parameter is utilised, which is the heading direction of the vehicle.

Consider the situation of one road with two directions as shown in Figure 9-2 (b), and consider that one vehicle on the road or a sensor on roadside (e.g., the sensor node B) needs to send an alert message to all vehicles that move in one direction. If the alert message is sent, then all the vehicles on the road in the two ways will receive this message. In addition, the information contained in the message are not of interest of the other routes receivers, as well as it directs the drivers intention and anxiety to unnecessary information which could be a reason for accidents.

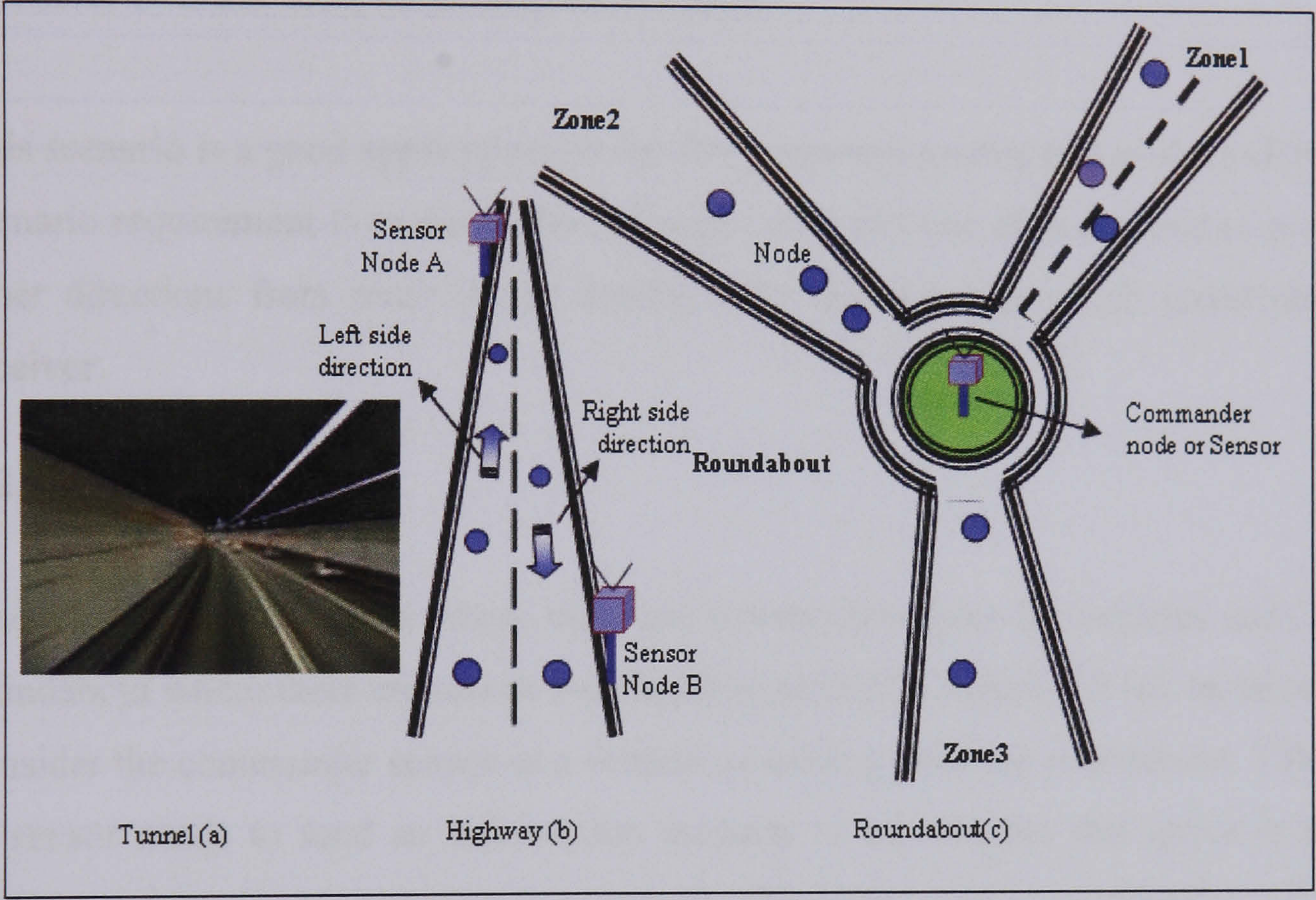


Figure 9-2: Scenarios of inter-vehicles

If the vehicles that move in one direction denoted as $rt-dir_1$ and have a heading direction angle θ_1, and vehicles that move in the opposite direction denoted as $rt-dir_2$ and have a heading direction angle θ_2. Consider the function that sends the alert message is $send(\theta)$. The function that is triggered when an alert message is received is $recv(\theta)$. Then, when a vehicle p_1 belong to $rt-dir_1$ sends an alert message $Alrt_1$ to another vehicle p_2 belonging to $rt-dir_1$ by triggering $send(\theta_1)$ function, and since the ad hoc networks operate in multiple access receiving, hence, all other vehicles in all directions ($rt-dir_1$ and $rt-dir_2$) will receive $Alrt_1$. Preventing other vehicles in

$rt-dir_2$ from receiving $Alrt_1$ is done formally by:

$$\forall p_1, p_2 \in rt-dir_1, q \in rt-dir_2, p_1 \leftrightarrow q, p_1 \leftrightarrow p_2 \Leftrightarrow p_1 \neq q, p_2$$

$$recv(\theta 1) \Rightarrow \begin{cases} drop(Alrt_1) & if\ \theta_q \neq \theta_1 \pm \delta \\ \\ Accept(Alrt_1) & if\ \theta_q \cong \theta_1 \pm \delta \end{cases}$$

Where, δ is the acceptable variation around θ_1.

This scenario is a good application for the first proposed routing protocol (HARP1) as the scenario requirement is to direct the message from only one direction and to prevent the other directions from receiving or dealing with this message which could disrupt the receiver.

9.2.2 Scenario Two

Another scenario could be where there are several directions for vehicles such as at the roundabout where there are one or more exist as shown in Figure 9-2 (c). In this situation, consider the commander sensor or a vehicle on exiting from the roundabout. This vehicle or sensor needs to send an information message to all vehicles that move in the same direction of the sender direction (e.g. zone1). The same as previous situation, all vehicles on all routes of the roundabout will unintentionally receive this message and deal with it as it is addressed to them.

Consider a commander sensor that is situated on the roundabout with number of exit routes n_{exit}. Each exit has one of the heading directions from the north $(\theta_1, \theta_2, ...\theta_{n_{exit}})$. The function that is triggered to send an alert message is $send(\theta_i)$ where i is the number of exit routes on the round about and has value $(1...n_{exit})$. The function that is triggered when an alert message is received is $recv(\theta_i)$. Here, the commander sensor has two options to send an alert message:

I) Either to send the alert message directed to all vehicles on one exit route on the roundabout.

II) Or to send the alert message directed to all vehicles on all exit routes on the roundabout.

In the first option, when a commander sensor CS_1 sends an alert message $Alrt_i$ to vehicles p_i belonging to $rt-dir_{i,i=1..n_{exit}}$ by triggering $send(\theta_i)$ function, and since the ad hoc networks operate in multiple access receiving, hence, all other vehicles in all other exit routes ($rt-dir_{j,j\neq i,j=1..n_{exit}}$) will receive $Alrt_i$. Preventing other vehicles in $rt-dir_{j,j\neq i,j=1..n_{exit}}$ from receiving $Alrt_1$ is done formally by:

$$\forall p_i \in rt-dir_{i,i=1..n_{exit}}, q_j \in rt-dir_j, i \neq j, cs_1 \leftrightarrow p_i, cs_1 \leftrightarrow q_j \Leftrightarrow p_i \neq q_j, cs_1 \rightarrow send(\theta_i)$$

$$k \rightarrow recv(\theta_i) \Rightarrow \begin{cases} drop(Alrt_i) & if \;\; \theta_k = q_j \neq \theta_i \pm \delta, k \in rt-dir_j, k \neq i \\ \\ Accept\;(Alrt_i) & if \;\; \theta_k \cong \theta_i \pm \delta \end{cases}$$

Where, δ is the acceptable variation around θ_i.

In the second option, when a commander sensor CS_1 sends an alert message $Alrt$ to vehicles $p_i, p_j, ... p_{n_{exit}}$ belonging to $rt-dir_{i,i=1..n_{exit}}$ by triggering $send(\theta)$ function, and since the ad hoc networks operate in multiple access receiving, hence, all vehicles in all exit routes ($rt-dir_{i,i=1..n_{exit}}$) that are within the transmission range of CS_1 will receive the $Alrt_i$ message. Formally:

$$\forall p_i \in rt-dir_{i,i=1..n_{exit}}, q_j \in rt-dir_j, i \neq j, cs_1 \leftrightarrow p_i, cs_1 \leftrightarrow q_j \Leftrightarrow p_i \neq q_j, cs_1 \rightarrow send(\theta)$$

$$k \rightarrow recv(\theta) \Rightarrow \begin{cases} drop(Alrt) \;\; if \;\; k, q_j \in rt-dir_j, q_j alreadyAccept(Alrt), k \neq j \\ \\ Accept(Alrt) \;\; if \;\; k, q_j \in rt-dir_j, q_j alreadydrop(Alrt), k \neq j \end{cases}$$

This scenario is good application example for the second routing protocol (HARP2) as the scenario requirement is to direct the message to certain number of direction such as at the roundabout.

9.2.3 Scenario Three

One more scenario/situation can be the underground trains or a tunnel with two directions (Figure 9-2 (a)). The difference between this scenario and the first scenario is that: if the ad hoc network used in such environments and such scenarios depends on GPS system to determine the geographical positions of vehicles, then such network in latter scenarios will be frozen and all network functionality will be ineffective.

In recognition to all above scenarios, the need to directional routing protocols or directional antennas is crucial in such environment. Directional antenna is costly since each vehicle and every sensor on the roadside requires having muti-directed antennas. Choudhury and Vaidya [72, 73] evaluate the performance of a reactive routing protocol for different scenarios using directional antennas, the outcome of their result is that by using directional antennas, ad hoc networks may achieve better performance and scenarios exist in which using omnidirectional antennas may be more appropriate. In addition, in the situation of the last explained scenario, the ad hoc network requires alternative information to be provided to routing protocols instead of geographical information.

9.3 SUMMARY

In this chapter, a framework about implementing and using mobile ad hoc network in the Telecare System was proposed in order to help elderly people. The problem, the requirement and the building environment for this framework were defined. In addition, the “inter-vehicle” application was explained as a case study for the proposed algorithms; since three scenarios are elaborated on to clarify the environment and the situations of implementing these schemes.

Chapter 10
Conclusions and Future Work

10.1 Conclusion

Rapid advances in the technology of wireless communication systems and small, lightweight, portable devices migrating into the field of mobile ad hoc networks. Designing communication protocols and applications for ad hoc networks is very challenging due to the absence of fixed infrastructure, the inevitable mobility, and constrained bandwidth.

Effectively delivering data packets and minimising connection breakdown and control packets overhead, while ensuring a route remains connected for the longest possible period are crucial in ad hoc networks. Mobility in wireless mobile ad hoc networks presents the most difficult challenge to routing protocol designers. Mobility causes frequent topology changes and route invalidation, which increase the signalling overhead required to establish routes, and thus affect the performance of the routing protocols. Therefore, routing protocols must construct and maintain multihop routes in dynamic ad hoc networks effectively and efficiently.

With the success of adopting the concept of heading direction angle of the nodes in mobile ad hoc network and in environments where other external routing information is absent, two new on-demand routing approaches for mobile ad hoc networks have been presented. In addition, a third new on-demand routing protocol has been presented with the availability of external routing information. These approaches have been shown to improve the route lifetime, reduce the control overhead and the effect of flooding in the network in addition to decreasing the effects of mobility.

In addition, a new Adaptive Centralised Location Service (ACLS) has been presented, which tracks mobile node locations. ACLS overcomes the main problems of centralised static servers in location service approaches such as the failure of the server, (which will lead to whole the system to cease functioning) and heavy load at a single server. In ACLS, the identity of the server is *a priori* unknown to the initiator of the location update message and the location request message. The addressing of servers is thus called anonymous addressing, because the receivers decide independently, based on current values of the node's parameters and on the contents of the message, whether they are the intended destination. Mostly the position of nodes determines whether they are the destination of a message. Several optimizations have been implemented in the ACLS algorithm in order to improve its efficiency and functionality of providing the requested location information as accurately as possible.

The main lesson learned from these studies is that:

- A better way to deal with mobility in mobile ad hoc networks is to get benefit from it rather than searching for ways to avoid it or to reduce its effects. In other words, a better solution for the side effects of mobility in ad hoc networks is to convert mobility from being burden to be beneficial by exploiting the positive side of it, which is the heading direction.
- More self-dependent the routing protocol, the more generalised it becomes for most applications. This means that, when the routing protocol depends on internal routing information, it also becomes more applicable in many other applications, whereas the more external dependencies for required routing information, more application specific it becomes.

The simulation results showed that exploiting the mobility patterns of nodes would allow routes to remain connected longer and overcome the effect of flooding technique and overhead in the network. This is achieved by selective forwarding, and elongating the lifetime of routes. Results also showed improvement in reduction of the effect of flooding in terms of routing discovery packets needed to deliver data packets with different mobility, speeds of nodes and different network size. Results have also shown that the ratio between the number of data packets delivered to the destinations to the number of all packets generated in the networks is higher in all schemes compared to the conventional AODV protocol, which is a result of choosing the longest path to the destination.

The studied approaches can be a solution to some of the problems occurring in ad hoc networks. For example, providing mechanisms to handle the frequent changes in the network topology due to mobility; and maintaining the long-lived multi-hop paths between two communicating nodes. Combining other routing protocols for mobile ad hoc networks can be applied to these schemes in order to improve the performance or QoS of these protocols in terms of protracting the lifetime of the communications.

Simulation results of ACLS algorithm showed that ACLS is a highly adaptive and scalable mechanism. The average of the Success Rate of Delivering the Location Update Packets (SRDLUP) is about 0.92 in terms of number of nodes. The SRDLUP rate at number of nodes equal to 50 is 0.993, which indicates that almost all location update packets are reached and received by servers. In terms of the scalability with the speed of nodes, results showed that the SRDLUP rate is approximately 100% with different values of speed.

Almost all location query request packets generated by the generator nodes have received replies about the location of requested nodes. In terms of mobility, the average value of the Success Rate of Delivering the Location Query Request Packets SRDLQRP is equal to 0.97, and the maximum value is 0.99.

The main lesson learned from these results is: using adaptive servers in mobile ad hoc networks instead of relying on some fixed and static servers gives much better performance in terms of adaptiveness and scalability and provides solution to the failures caused by the servers (e.g., server goes down, server moves outside its location, etc).

10.2 Future Work

With respect to future work, in the first three designed protocols a deeper investigation of choosing the number of zones that the node's neighbours are grouped into according to the density and mobility of the network is required in order to improve the performance of these protocols. In addition, investigating the number of selected neighbours to forward the packet will be a further step to enhance the performance. Furthermore, applying these schemes on other existing protocols to improve their performance is the main aim for future work.

In ACLS location service protocol, in order to compare the performance of ACLS with other location service protocols, the results to be achieved must be coherent. Such comparisons could not be performed because of two reasons. The first reason is that the centric server approach used in ad hoc networks is a static server. In the static server, the mobile ad hoc network relies on fixed infrastructure, (the single fixed server). In the proposed approach, the servers are mobile and dynamic. The server in this approach, at a specific time, ceases to become the server and another node that has specific characteristics is converted to a server. The second reason is that the paradigm of *anonymous addressing* is relatively new and therefore has rarely been addressed in the literature.

Some other future research directions, which are the interesting challenges in the ad hoc network area, include:

- Multicast routing protocols design
- MAC layer protocols development
- Efficient load balancing approaches
- End-to-End Quality of Service (QoS) provision
- Power efficient protocols design
- Cross-layers design for wireless networks
- Multipath routing approaches development
- End-to-End security and privacy
- Interoperation with hybrid networks (wired/cellular/ad hoc networks)
- Carry on the work in telecare system proposed in this thesis.

References

[1] Y.-B Ko and N. H. Vaidya, "Location-Aided Routing (LAR) in mobile ad hoc networks", Wireless Networks 6, 2000.

[2] E. M. Royer, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communication April 1999.

[3] C. Siva Ram Murthy and B.S. Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols", book, ISBN 0-13-147023-X, first printing, 2004

[4] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," in Proc. IEEE/ACM Mobicom'98, Oct. 1998.

[5] C. E. Perkins, E. M. Royer, S. R. Das, and M. K. Marina, "Performance comparison of two on-demand routing protocols for ad hoc networks," IEEE Pers. Commun., Feb. 2001.

[6] A. Bruce McDonald and T. Znati, "A Mobility-Based Framework for Adaptive Clustering in Wireless Ad-Hoc Networks", IEEE Journal on Selected Areas in Communication, Vol. 17, No. 8, August 1999.

[7] S. Basagni, D. Turgut and S. K. Das., "Mobility-adaptive protocols for managing large ad hoc networks", Proceedings of IEEE International Conference on Communications (ICC), Jun 2001.

[8] W. Su, S-J. Lee and M. Gerla, "Mobility Prediction in Wireless Networks", In Proceedings of IEEE MILCOM 2000, Vol. 1, Los Angelas, CA, October 2000.

[9] R. Dube, C.D. Rais, K-Y.Wang and S.K. Tripathi, "Signal Stability-Based Adaptive Routing (SSA) for Ad-Hoc Mobile Networks", IEEE Personal Communications journal, February 1997.

[10] C-K. Toh, "Associativity-Based Routing for Ad-Hoc Networks", Wireless Personal Communications Journal, Special Issue on Ad-Hoc Networks, Vol. 17, No. 8, August 1999.

[11] C. E. Perkins, E. M. Belding-Royer, S. R. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", (Internet-draft), in: Mobile Ad-hoc Network (MANET) Working Group, IETF, 17 February 2003.

[12] M. Sheng, J. Li, and Y. Shi, "Relative Degree Adaptive Flooding Broadcast Algorithm for Ad Hoc Networks", IEEE Transactions on broadcasting, VOL. 51, NO. 2, JUNE 2005

[13] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad-hoc wireless networks," in Mobile Comput., T. Imielinski and H. Korth, Eds: Kluwer, 1996.

[14] Y.-B. Ko and N.H. Vaidya, "Location-Aided Routing (LAR) in Mobile Ad Hoc Networks", Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM), Dallas, TX, October 1998.

[15] M. Joa-Ng and I.-T. Lu, "A Peer-to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks", IEEE Journal on Selected Areas in Communications, special issue on Wireless Ad Hoc Networks, vol. 17, no. 8, August 1999.

[16] W. Su and M. Gerla, "IPv6 Flow Handoff in Ad Hoc Wireless Networks Using Mobility Prediction", Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM), Rio de Janeiro, Brazil, December 1999.

[17] B. Karp and H.T. Kung, "Greedy Perimeter Stateless Routing for Wireless Networks", in Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 2000), Boston, MA, August, 2000.

[18] B. Karp, "Geographic Routing for Wireless Networks", PhD thesis, Harvard University, Cambridge, MA, October 2000.

[19] M. Al-Akaidi, M. Alchaita, J. Ivins, "Heading Routing Protocols: Mobility-Based Routing For Ad-Hoc Networks", The IEE, 3G 2005, Sixth International Conference on 3G and Beyond - 3G 2005, 07-09 November 2005,

[20] M. Alchaita, M. Al-Akaidi, J. Ivins, "New On-demand Routing Approaches for Ad Hoc Networks", PGNet 2005, sixth annual postgraduate symposium, the convergence of telecommunications, networking and broadcasting, 27th-28th June 2005.

[21] P. H. Dana, "Global Positioning System Overview",

URL: http://www.colorado.edu/geography/gcraft/notes/gps/gps_f.html, 2000.

[22] G. Dommety and R. Jain, Potential networking applications of global positioning systems (GPS), Technical report TR-24, The Ohio State University, 1996.

[23] M. Alchaita, M. Al-Akaidi, M. Aziz, "APPLICATION OF A NEW ROUTING PROTOCOL IN TELECARE SYSTEM", PGBIOMED05, IEEE EMBSS UKRI Postgraduate Conference on Biomedical Engineering and Medical Physics, 18-20 July 2005.

[24] M. Abolhasan, T. Wysocki, E. Dutkiewicz, "A review of routing protocols for mobile ad hoc networks", Ad Hoc Networks journal, Elsevier Science, Vol. 2, 2004.

[25] S. Basagni, I. Chlamtac, V.R. Syrotivk, B.A. Woodward, "A distance routing effect algorithm for mobility (DREAM)", Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom'98), Dallas, TX, 1998.

[26] A. Udaya Shankar, C. Alaettinoglu, I. Matta, K. Dussa-Zieger, "Performance comparison of routing protocols using MaRS: distance-vector versus link-state", in: Proceedings of the 1992 ACM SIGMETRICS and PERFORMANCE '92 Int'l. Conf. on Measurement and Modeling of Computer Systems, Newport, RI, USA, 1–5 June 1992.

[27] R.E. Bellman, "Dynamic Programming", Princeton University Press, Princeton, NJ, 1957.

[28] L.R. Ford and D.R. Fulkerson, "Flows in Networks", Princeton University Press, Princeton, NJ, 1962.

[29] C.E. Perkins, T.J. Watson, "Highly dynamic destination sequenced distance vector routing (DSDV) for mobile computers", in: ACM SIGCOMM'94 Conference on Communications Architectures, London, UK, 1994.

[30] S. Murthy and J.J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks", ACM/Baltzer Mobile Networks and Applications, special issue on Routing in Mobile Communications Networks, vol. 1, no. 2, October 1996.

[31] S. Murthy J.J. Garcia-Luna-Aceves, "A routing protocol for packet radio networks", in: Proceedings of the First Annual ACM International Conference on Mobile Computing and Networking, Berkeley, CA, 1995.

[32] T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, a. Qayyum et L. Viennot, "Optimized Link State Routing Protocol", IEEE INMIC Pakistan 2001.

[33] G. Pei, M. Gerla, T.-W. Chen, "Fisheye State Routing in Mobile Ad Hoc Networks" ICDCS Workshop on Wireless Networks and Mobile Computing, 2000

[34] G. Pei, M. Gerla, T.-W. Chen, "Fisheye State Routing: A Routing Scheme for Ad Hoc Wireless Networks", Proceedings of the IEEE International Conference on Communications (ICC), New Orleans, LA, June 2000.

[35] J.J. Garcia-Luna-Aceves and M. Spohn, "Source-Tree Routing in Wireless Networks", Proceedings of the IEEE International Conference on Network Protocols (ICNP), Toronto, Canada, October, 1999.

[36] T.-W. Chen and M. Gerla, "Global State Routing: A New Routing Scheme for Ad-hoc Wireless Networks," Proceedings of the IEEE International Conference on Communications (ICC), Atlanta, GA, June 1998.

[37] C.-C. Chiang, H. K. Wu, W. Liu, and M. Gerla, "Routing in clustered multihop mobile wireless networks with fading channel", in: Proceedings of IEEE SICON, April 1997.

[38] D. Johnson, D. Maltz, and Y. Hu., "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", IETF MANET Working Group, Internet Draft, draft-ietf-manet-dsr-10.txt, 19 July 2004.

[39] V.D. Park, M.S. Corson, A highly adaptive distributed routing algorithm for mobile wireless networks, Proceedings of the IEEE Conference on Computer Communications (INFOCOM), Kobe, Japan, April 1997, pp.1405-1413.

[40] V. PARK, S. CORSON, "Temporally-Ordered Routing Algorithm (Tora) Version 1", Internet Draft, draft-ietf-manet-tora-spec- 03.txt, work in progress, June 2001.

[41] C. Toh, "A novel distributed routing protocol to support ad-hoc mobile computing", IEEE 15th Annual International Phoenix Conf., 1996.

[42] D. B. Johnson, "Routing in Ad Hoc Networks of Mobile Hosts", Proceedings of the IEEE workshop on Mobile Computing Systems and Applications, December 1994.

[43] D.A. Maltz, J. Broch, J. Jetcheva, and D.B. Johnson, "The Effects of On-Demand Behavior in Routing Protocols for Multihop Wireless Ad Hoc Networks", IEEE Journal on Selected Areas in Communications, special issue on Wireless Ad Hoc Networks, vol. 17, no. 8, August 1999.

[44] IEEE Computer Society LAN MAN Standards Committee. "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11-1999, New York, 1999.

[45] X. Zou, B. Ramamurthy, "Routing Techniques in Wireless Ad Hoc Networks - Classification and Comparison", The Sixth World Multiconference on Systemics, Cybernetics, and Informatics, SCI 2002, Volume IV, Orlando, Florida, USA, 15-18. July 2002

[46] Z. J. Haas, M. R. Pearlman, and P. Samar, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks", draft-ietf-manet-zone-zrp-04.txt, July, 2002

[47] R. Sivakumar, P. Sinha, and V. Bharghavan, "CEDAR: a Core-Extraction Distributed Ad hocRouting algorithm", IEEE Journal On Selected Areas In Communication, Vol 17, No 8, August 1999.

[48] M. Gerla, G. Pei, S.-J. Lee, "Wireless, Mobile Ad-Hoc Network Routing", Proceedings of the ACM/IEEE WINLAB/Berkeley FOCUS, New Brunswick, NJ, May 1999.

[49] S. Ramanathan and M. Streenstrup, "A Survey of Routing Techniques for Mobile Communication Networks", ACM/Baltzer Mobile Networks and Applications, special issue on Routing in Mobile Communications Networks, vol. 1, no. 2, October 1996.

[50] Mobile Ad-hoc Networks (MANET) Working Group. http://www.ietf.org/html.charters/manet-charter.html.

[51] M. Gerla, X. Hong, Li Ma, "Landmark Routing Protocol (LANMAR) for Large Scale Ad Hoc Networks", draft-ietf-manet-lanmar-03.txt, IETF MANET Working Group, INTERNET-DRAFT, June 17, 2002

[52] M. Jiang, J. Li, Y.C. Tay, "Cluster Based Routing Protocol (CBRP)", draft-ietf-manet-cbrp-spec-01.txt, IETF MANET Working Group, INTERNET-DRAFT 14 August 1999

[53] E.D. Kaplan, "Understanding the GPS: Principles and Applications", Artech House, Boston, MA, February 1996.

[54] P. H. Dana, "Global Positioning System Overview", URL: http://www.colorado.edu/geography/gcraft/notes/gps/gps_f.html, 2000.

[55] G. Dommety and R. Jain, "Potential networking applications of global positioning systems (GPS)", Technical report TR-24, The Ohio State University, 1996.

[56] J. Li, J. Jannotti, D.S.J. De Couto, D.R. Karger, and R. Morris, "A Scalable Location Service for Geographic Ad Hoc Routing", Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM), Boston, MA. August 2000.

[57] Yu J.Y., Chong P.H.J., "A survey of clustering schemes for mobile ad hoc networks", Communications Surveys & Tutorials, IEEE, Volume 7, Issue 1, First Qtr. 2005.

[58] A. B. MaDonald and T. F. Znati, "A Mobility-based Frame Work for Adaptive Clustering in Wireless Ad Hoc Networks", IEEE JSAC, vol. 17, Aug. 1999.

[59] C. R. Lin and M. Gerla, "Adaptive Clustering for Mobile Wireless Networks", IEEE JSAC, vol. 15, Sept. 1997.

[60] T.-C. Hou and T. J. Tsai, "An Access-Based Clustering Protocol for Multihop Wireless Ad Hoc Networks," IEEE JSAC, vol. 19, no. 7, July., 2001.

[61] C.-C. Chiang et al., "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," in Proc. IEEE SICON'97, 1997.

[62] P. Basu, N. Khan, and T. D. C. Little, "A Mobility Based Metric for Clustering in Mobile Ad Hoc Networks," in Proc. IEEE ICDCSW' 01, Apr. 2001.

[63] A. D. Amis and R. Prakash, "Load-Balancing Clusters in Wireless Ad Hoc Networks," in Proc. 3rd IEEE ASSET'00, Mar. 2000.

[64] K. X. Xu, X. Y. Hong, and M. Gerla, "An Ad Hoc Network with Mobile Backbones", Proc. IEEE ICC'2002, vol. 5, Apr.–May 2002.

[65] U. C. Kozat et al., "Virtual Dynamic Backbone for Mobile Ad Hoc Networks", Proc. IEEE ICC'01, vol. 1, June 2001.

[66] X. Cheng and D.-Z. Du.,"Virtual backbone-based routing in multihop ad hoc wireless networks", Technical Report 002, University of Minnesota, June 2002.

[67] K. M. Alzoubi, P.-J. Wan, and O. Frieder, "Distributed heuristics for connected dominating set in wireless ad hoc networks", IEEE ComSoc/KICS Journal on Communication Networks, 4(1):22--29, 2002.

[68] S. Mikko, "Measuring the Effects of Mobility on Reactive Ad Hoc Routing Protocols", Master's Thesis, Helsinki University of Technology, April, 2004.

[69] T. Larsson and N. Hedman, "Routing protocols in wireless ad-hoc networks - a simulation study", Master's Thesis, Luleå Tekniska Universitet, 1998.

[70] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek, and M. Degermark, "Scenario-based performance analysis of routing protocols for mobile ad-hoc networks", In 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom), pages 195–206, Seattle Washington, August 1999.

[71] D. Turgut, S.K. Das, M. Chatterjee, "Longevity of Routes in Mobile Ad hoc Networks", Proc. IEEE VTC, Rhodes, Greece, spring 2001.

[72] R. Roy Choudhury and Nitin Vaidya, "Ad Hoc Routing Using Directional Antennas", Technical Report, August 2002.

[73] R. R. Choudhury and N. Vaidya, "Impact of Directional Antennas on Ad Hoc Routing", Recipient of the Best Paper Award at the Eighth International Conference on Personal Wireless Communication (PWC), Venice, September 2003.

[74] T. Camp, J. Boleng, and V. Davies. "A survey of mobility models for ad hoc network research", Wireless Communications and Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking, 2002.

[75] M. Sanchez and P. Manzoni, "A java-based ad hoc networks simulator", Proceedings of the SCS Western Multiconference Web-based Simulation Track, Jan. 1999.

[76] D. Son, A. Helmy, B.Krishnamachari, "The Effect of Mobility-Induced Location Errors on Geographic Routing in Mobile Ad Hoc and Sensor Networks: Analysis and

Improvement Using Mobility Prediction", IEEE Transactions on Mobile Computing, Volume: 03, Issue: 3, July 2004.

[77] X. Hong, M. Gerla, G. Pei, and C. C. Chiang, "A Group Mobility Model for Ad Hoc Wireless Networks", In Proc. ACM/IEEE MSWiM'99, Seattle, WA, August 1999.

[78] K. Blakely and B. Lowekamp, "A structured group mobility model for the simulation of mobile ad hoc networks", in Proceedings of the Second International Workshop on Mobility Management and Wireless Access Protocols, Philadelphia, PA, USA, 2004.

[79] M. Musolesi , S. Hailes , C. Mascolo, "An ad hoc mobility model founded on social network theory", In Proceedings of the 7th ACM/IEEE International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM 2004). October 2004.

[80] G. Lin, G. Noubir, and R. Rajamaran, "Mobility models for ad-hoc network simulation", In Proceedings of IEEE Infocom, 2004.

[81] W. Su, S-J. Lee and M. Gerla, "Mobility Prediction and Routing in Ad Hoc Wireless Networks", International Journal of Network Management, Wiley and Sons, 2000.

[82] R. Chellappa Doss, A. Jennings, N. Shenoy, "A REVIEW OF CURRENT MOBILITY PREDICTION TECHNIQUES FOR AD HOC NETWORKS", Proceeding of the 4th IASTED International Multi-Conference on Wireless and Optical Communications (WOC), July 8 – 10, 2004.

[83] X. Luo, T. Camp, W. Navidi, "Predictive Methods for Location Services in Mobile Ad Hoc Networks", 19th IEEE International, Parallel and Distributed Processing Symposium, 2005.

[84] H. Samarth, and K. Nahrstedt, "Predictive Location-Based QoS Routing in Mobile Ad Hoc Networks", In Proceedings of IEEE International Conference on Communications, 2002.

[85] D. A. Maltz. "On-Demand Routing in Multi-hop Wireless Mobile Ad Hoc Networks", PhD thesis, Carnegie Mellon University, 2001. http://www.monarch.cs.cmu.edu/monarchpapers /maltz-thesis.ps.gz.

[86] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen and J.-P. Sheu, "The broadcast storm problem in a mobile ad hoc network", Proc. MOBICOM, Seattle, Aug. 1999, pp. 151-162.

[87] Kumar Banka, R. Guoliang Xue, "Angle routing protocol: location aided routing for mobile ad-hoc networks using dynamic angle selection.", IEEE Milcom'2002 Conference, 2002.

[88] S. Kurkowski, T. Camp, M. Colagrosso, "MANET Simulation Studies: The Incredibles," ACM SIGMOBILE Mobile Computing and Communication Review, Vol. 9, Issue 4 October, 2005.

[89] The network simulator NS2 and Nam home page, http://www.isi.edu/nsnam/.

[90] Bruce Tuch. Development of WaveLAN, an ISM Band Wireless LAN. AT&T Technical Journal,72(4):27–33, July/August 1993.

[91] B. Liang and Z. Haas, "Virtual Backbone Generation and Maintenance in Ad Hoc Network Mobility Management", In INFOCOM, 2000.

[92] Gawk: Effective AWK Programming, The GNU Awk User's Guide, home page: http://www.gnu.org/software/gawk/manual/

[93] Solid State Electronics Center, home page, http://www.ssec.honeywell.com/magnetic/.

[94] P. Samar, S. B. Wicker, "On the behavior of communication links of a node in a multi-hop mobile environment", MobiHoc 2004.

[95] M Al-Akaidi and M Alchaita, "Mobility-Aware Routing Algorithm For Multi-Hop Ad-Hoc Wireless Networks", SSD'05, the Third IEEE International Conference on Systems, Signals & Devices, Sousse, Tunisia, 2005

[96] M Al-Akaidi and M Alchaita, "New Heading Directional Angle Routing Protocols For Mobile Ad Hoc Networks", IEE, Fifth International Conference on 3G Mobile Communication Technologies, 18 – 20 October, London, Uk.2004.

[97] A. T. Helmi Abd El-Nabi, "Modeling and simulation of routing protocol for ad hoc networks combining queuing network analysis and ANT colony algorithms", PhD dissertation, University of Duisburg-Essen, April 28, 2005

[98] M. Särelä, "Measuring the Effects of Mobility on Reactive Ad Hoc Routing Protocols", Helsinki University of Technology Laboratory for Theoretical Computer Science, Research Reports 91, 2004.

[99] A. A. Hamidian, "A Study of Internet Connectivity for Mobile Ad Hoc Networks in NS 2", thesis, department of communication systems, lund university, January 2003.

[100] S. McCanne, S. Floyd, "Network Simulator", http://www.isi.edu/nsnam/ns/, Kevin Fall, Kannan Varadhan, and the VINT project.

[101] "Global Mobile Information System Simulation GloMoSim", home page, See URL: http://pcl.cs.ucla.edu/projects/glomosim/

[102] OPNET Modeler, home page, See URL: http://www.opnet.com/products/modeler/home.html

[103] R. Bagrodia and W. Liao. Maisie, "A language for design of efficient discrete event simulation computer networks", IEEE Transactions on Software Engineering, April 1994.

[104] K. Fall and K. Varadhan, "NS Notes and Documentation". The VINT Project, UC Berkeley, LBL, USC/ISI, and Xerox PARC, January 1999. Available from http://wwwmash.cs.berkeley.edu/ns/.

[105] B. Ryu, T. Andersen, M. Ahmed, T. Elbatt, A. Peterson, "Research Tools for 3-D Mobile Ad-hoc Networking with Directional Antenna", HRL Laboratories, LLC, 2002.

[106] E. Hyytiä and J. Virtamo, "Random waypoint model in n-dimensional space". Operations Research Letters, vol. 33/6, 2005

[107] N. Guba and T. Camp, "GLS: a location service for an ad hoc network". In Proceedings of the Grace Hopper Celebration (GHC '02), 2002.

[108] I. Stojmenovic, "Home Agent Based Location Update and Destination Search Schemes in Ad Hoc Wireless Networks," Tech. rep. TR-99-10, Comp. Science, SITE, Univ. Ottawa, Sept. 1999.